UNCLASSIFIED

Windows Vista Security Technical Implementation Guide

Version: 6

Release: 1.18

25 Jun 2010

STIG.DOD.MIL

Sort Order: Group ID (Vulid), ascending order
Notice: Developed_by_DISA_for_the_DoD
Description: The Windows Vista Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements were developed from DoD consensus, as well as the Windows Vista Security Guide and security templates published by Microsoft Corporation.

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist

Secret System= SECRET Checklist
Top Secret System = SECRET Checklist

Group ID (Vulid): V-1070
Group Title: Physical security
Rule ID: SV-29618r1_rule
Severity: CAT II
Rule Version (STIG-ID): 1.001
Rule Title: Physical security of the Automated Information System (AIS) does not meet DISA requirements.

Vulnerability Discussion: Inadequate physical protection can undermine all other security precautions utilized to protect the system. This can jeopardize the confidentiality, availability, and integrity of the system. Physical security of the AIS is the first line protection of any system.

Responsibility: System Administrator
IAControls: PECF-1

Check Content:
Interview the SA to determine if equipment is located in an access controlled area.

Note: Servers will be located in rooms, or locked cabinets, that are accessible only to authorized systems personnel. Authorized user access should be verified at two points (i.e. building access and server room). User workstations containing sensitive data should be in access controlled areas.

Fix Text: Relocate equipment to a controlled access area.

Group ID (Vulid): V-1072
Group Title: Shared User Accounts
Rule ID: SV-29622r1_rule
Severity: CAT II
Rule Version (STIG-ID): 1.008
Rule Title: Shared user accounts are permitted on the system.

Vulnerability Discussion: Shared accounts do not provide individual accountability for system access and resource usage.

Responsibility: System Administrator
IAControls: IAGA-1

Check Content:

Interview the SA to determine if any shared accounts exist.

Any shared account must be documented with the IAO. Documentation should include the reason for the account, who has access to this account, and how the risk of using a shared account (which provides no individual identification and accountability) is mitigated.

Note: As an example, a shared account may be permitted for a help desk or a site security personnel machine, if that machine is stand-alone and has no access to the network.

Fix Text: Remove any shared accounts that do not meet the exception requirements listed.

Group ID (Vulid): V-1073
Group Title: Approved Service Packs
Rule ID: SV-29339r1_rule
Severity: CAT II
Rule Version (STIG-ID): 2.005
Rule Title: The current, approved service pack is not installed.

Vulnerability Discussion: Failure to install the most current Windows service pack leaves a system vulnerable to exploitation. Current service packs correct known security and system vulnerabilities. If a Windows OS is at an unsupported service pack this will be upgraded to a Category I finding since new vulnerabilities may not be patched.

Documentable: YES
Security Override Guidance:
Unsupported Service Packs will be upgraded to a Category I finding.

Responsibility: System Administrator
IAControls: VIVM-1

Check Content:
From the menu bar click “Start” and then “Run”.
Type “winver.exe” in the dialog box and click OK.
If the "About Windows" box does not display the current approved service pack, then this is a finding.

Current Required Service Packs
Vista – SP2

Note: Application of new Service Packs should be thoroughly tested before deploying in a production environment.

Severity Override: Unsupported Service Packs will be upgraded to a Category I finding. This includes the following:

Windows Vista - SP0

Documentable Explanation: Some managed systems such as DMS and GCSS receive service pack updates via system releases. In this case the current approved application release should be installed.

Fix Text: Install the current approved service pack.

Rule ID: SV-29341r1_rule
Severity: CAT I

Rule Version (STIG-ID): 2.005
Rule Title: The current, approved service pack is not installed.

Vulnerability Discussion: Failure to install the most current Windows service pack leaves a system vulnerable to exploitation. Current service packs correct known security and system vulnerabilities. If a Windows OS is at an unsupported service pack this will be upgraded to a Category I finding since new vulnerabilities may not be patched.

Documentable: YES
Security Override Guidance:
Unsupported Service Packs will be upgraded to a Cat I finding.

Responsibility: System Administrator
IAControls: VIVM-1

Check Content:
From the menu bar click “Start” and then “Run”.
Type “winver.exe” in the dialog box and click OK.
If the "About Windows" box does not display the current approved service pack, then this is a finding.

Current Required Service Packs
Vista – SP2

Note: Application of new Service Packs should be thoroughly tested before deploying in a production environment.

Severity Override: Unsupported Service Packs will be upgraded to a Category I finding. This includes the following:

Windows Vista - SP0

Documentable Explanation: Some managed systems such as DMS and GCSS receive service pack updates via system releases. In this case the current approved application release should be installed.

Fix Text: Install the current approved service pack.

Group ID (Vulid): V-1074
Group Title: Approved DOD Virus Scan Program
Rule ID: SV-29469r1_rule
Severity: CAT I
Rule Version (STIG-ID): 5.007
Rule Title: An approved DOD virus scan program is not used and/or updated.

Vulnerability Discussion: This is a Category 1 finding because Virus scan programs are a primary line of defense against the introduction of viruses and malicious code that can destroy data and even render a computer inoperable. Utilizing the most current virus scan program provides the ability to detect this malicious code before extensive damage occurs. Updated virus scan data files can help protect a system, because new viruses are identified by the software vendors on a monthly basis.

False Positives:
The scripts check for McAfee and Symantec Antivirus, corporate and client editions. Due to variation of installations, manual checks may be required for verifying Anti-Virus compliance.

False Negatives:
E-Mail versions of anti-virus software are not acceptable as protection for Windows operating systems. However, both the E-Mail anti-virus software and the operating system anti-virus software can coexist and run on the same

system.

Documentable: YES
Responsibility: System Administrator
IAControls: ECVP-1

Check Content:
Note: The Gold Disk checks for McAfee and Symantec Antivirus, corporate and client editions. Due to variation of installations, manual checks may be required for verifying antivirus compliance.

V0019910 has been added as part of the Desktop STIG Update which specifically looks at McAfee and Symantec AV signature files. If you have these programs, address them with that requirement and mark this one as N/A.

If none of the following products are installed and supported at an appropriate maintenance level, then this is a finding:

Symantec Antivirus at the following level is not installed:
Corporate Edition Version 9.0.6 or higher
Corporate Edition Version 10.x or higher
Endpoint Protection Version 11.0 or higher

McAfee's Antivirus Version 8.0 or higher is not installed.

And
The antivirus signature file is out of date.
If the anti virus program signature file is not dated within the past 7 days, then this is a finding.

Note: The version numbers and the date of the signature file can generally be checked by starting the antivirus program from the toolbar icon or from the Start menu. The information may appear in the antivirus window or be available in the Help > About window. The location varies from product to product.

Note: E-mail versions of antivirus software are not acceptable as protection for Windows operating systems. However, both the e-mail antivirus software and the operating system antivirus software can coexist and run on the same system.

Documentable Explanation: If a recognized antivirus product, such as Innoculator or another product is installed and has a current signature file, then this would still be a finding, but the severity code should be reduced to a Category III.

Fix Text: Configure the system with supported, DoD-approved virus scanning software. Ensure that the signature file is current.

Group ID (Vulid): V-1075
Group Title: Display Shutdown Button
Rule ID: SV-29590r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.007
Rule Title: The system allows shutdown from the logon dialog box.

Vulnerability Discussion: Preventing display of the shutdown button in the logon dialog box may encourage a hard shut down with the power button. The Shutdown button will be displayed per the FDCC. (Howevery, displaying the shutdown button may allow individuals to shut down a system anonymously.)

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:
FDCC XP and Vista - Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for "Shutdown: Allow shutdown without having to log on" is not set to "Enabled", then this is a finding.

Fix Text: FDCC XP and Vista - Configure the policy as specified in the manual check to allow the system to be shutdown without logging on.

Group ID (Vulid): V-1076
Group Title: System Recovery Backups
Rule ID: SV-29626r1_rule
Severity: CAT III
Rule Version (STIG-ID): 1.013
Rule Title: System information backups are not created, updated, and protected according to DISA requirements.

Vulnerability Discussion: Recovery of a damaged or compromised system in a timely basis is difficult without a system information backup. A system backup will usually include sensitivie information such as user accounts that could be used in an attack. As a valuable system resource, the system backup should be protected and stored in a physically secure location.

Responsibility: System Administrator
IAControls: CODB-1

Check Content:
Interview the SA to determine if system recovery backup procedures are in place that comply with DoD requirements.

Any of the following would be a finding:

•The site does not maintain emergency system recovery data.
•The emergency system recovery data is not protected from destruction and stored in a locked storage container.
•The emergency system recovery data has not been updated following the last system modification.

Fix Text: Implement data backup procedures that comply with DoD requirements.

Group ID (Vulid): V-1077
Group Title: Incorrect ACLs for event logs
Rule ID: SV-15087r3_rule
Severity: CAT II
Rule Version (STIG-ID): 2.001
Rule Title: ACLs for event logs do not conform to minimum requirements.

Vulnerability Discussion: Event logs are susceptible to unauthorized, and possibly anonymous, tampering if proper ACLs are not applied.

False Positives:
The "Auditors" group may appear as a finding. This is because the name of the group is left to the site. If an auditors group is present, its presence doesn't constitute a finding.

Responsibility: System Administrator
IAControls: ECTP-1

Check Content:
Set the permissions on the event logs (application.evtx, security.evtx and system.evtx) to the following.

Account Assignment Permission
Administrators Read and Execute
(Auditor's group) Full
SYSTEM Full
Eventlog Full

By default, all are found in the "%SystemRoot%\SYSTEM32\WINEVT\LOGS" directory. They may have been moved to another folder.

Note: See V-1137 for the Auditors group requirement.

The "Auditors" group may appear in the Gold Disk output as a finding. This is because the name of the group is left to the sites. If an auditors group is present, its presence doesn't constitute a finding.

If the permissions for these files are not as restrictive as the ACL listed, then this is a finding.

Fix Text: Set the ACL permissions on the event logs as defined in the manual check.

Group ID (Vulid): V-1080
Group Title: File Auditing Configuration
Rule ID: SV-29473r1_rule
Severity: CAT II
Rule Version (STIG-ID): 2.007
Rule Title: File-auditing configuration does not meet minimum requirements.

Vulnerability Discussion: Improper modification of the core system files can render a system inoperable. Further, modifications to these system files can have a significant impact on the security configuration of the system. Auditing of significant modifications made to the system files provides a method of determining the responsible party.

False Positives:
Automated checking sometimes reports this as a false finding. If a manual review of a questionable finding shows auditing to be set correctly, then this would not be a finding.

Responsibility: System Administrator
IAControls: ECAR-1, ECAR-2, ECAR-3

Check Content:
If system-level auditing is not enabled, or if the system and data partitions are not installed on NTFS partitions, then mark this as a finding.

Open Windows Explorer and use the file and folder properties function to verify that the audit settings on each partition/drive is configured to audit all "failures" for the "Everyone" group.

If any partition/drive is not configured to at least the minimum requirement, then this is a finding.

Fix Text: Configure auditing on each partition/drive to audit all "Failures" for the "Everyone" group.

Group ID (Vulid): V-1081
Group Title: NTFS Requirement
Rule ID: SV-29477r1_rule
Severity: CAT I
Rule Version (STIG-ID): 2.008
Rule Title: Local volumes are not formatted using NTFS.

Vulnerability Discussion: This is a category 1 finding because the ability to set access permissions and audit critical directories and files is only available by using the NTFS file system. The capability to assign access permissions to file objects is a DOD policy requirement.
The FAT file system only provides the capability to make files read-only and hidden. The capability to change these attributes is not restricted to any users. An unauthorized individual could boot the machine from a floppy disk and gain full and unrecorded access to file data.

Documentable: YES
Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open Windows Explorer and use the Properties function on each fixed local partition/drive to examine the File System specified on the General Tab.

If the File System does not specify NTFS, then this is a finding.

Documentable Explanation: Some hardware vendors create a small FAT partition to store troubleshooting and recovery data. No other files should be stored here. This requirement should be documented with the IAO.

Fix Text: Format all partitions/drives to use NTFS.

Group ID (Vulid): V-1084
Group Title: Clear System Pagefile
Rule ID: SV-28975r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.003
Rule Title: System pagefile is cleared upon shutdown.

Vulnerability Discussion: This check verifies that Windows is not configured to wipe clean the system page file during a controlled system shutdown per the FDCC.

Responsibility: System Administrator
IAControls: ECRC-1

Check Content:
FDCC XP and Vista - Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Shutdown: Clear virtual memory pagefile” is not set to “Disabled”, then this is a finding.

Fix Text: Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. Set the value for “Shutdown: Clear virtual memory pagefile” to “Disabled”.

Group ID (Vulid): V-1085
Group Title: Removable media devices - Floppies
Rule ID: SV-28976r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.006
Rule Title: Floppy media devices are not allocated upon user logon.

Vulnerability Discussion: This check verifies that Windows is configured to not limit access to floppy drives when a user is logged on locally per the FDCC.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Devices: Restrict floppy access to locally logged-on user only” is not set to “Disabled”, then this is a finding.

Fix Text: Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. Set the value for “Devices: Restrict floppy access to locally logged-on user only” to “Disabled”.

Group ID (Vulid): V-1088
Group Title: Registry Key Auditing
Rule ID: SV-29630r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.010
Rule Title: Registry key auditing configuration does not meet minimum requirements.

Vulnerability Discussion: Improper modification of the Registry can render a system useless. Modifications to the Registry can have a significant impact on the security configuration of the system. Auditing of significant modifications made to the Registry provides a method of determining the responsible party.

False Positives:
Sometimes audit settings may be incorrectly reported as findings. If a manual review reveals that they are set properly, then this would not be a finding.

Responsibility: System Administrator
IAControls: ECAR-3

Check Content:
If system-level auditing is not enabled, then mark the check in this section as “FINDING.”

Run regedt32.
Navigate to the Hkey_Local_Machine\Software and Hkey_Local_Machine\System keys.
On the menu bar, select “Security”, then select “Permissions” (2000) or "Edit" then "Permissions.
Click on the “Advanced” button.
Select the Auditing tab.
Highlight an ‘Auditing Entry” and click the view button.

If the Everyone group, at a minimum, is not being audited for all failures, then this is a finding.

Fix Text: Configure the Hkey_Local_Machine\Software and Hkey_Local_Machine\System keys to audit the Everyone Group for all failures. Audit settings should be propogated to subkeys.

Group ID (Vulid): V-1089
Group Title: Legal Notice is not Configured
Rule ID: SV-29633r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.011
Rule Title: Legal notice is not configured to display before console logon.

Vulnerability Discussion: Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

False Positives:
Legal notices can vary considerably between organizations. As long as it contains the required elements, it would not be a finding.

Responsibility: System Administrator
IAControls: ECWM-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Interactive Logon: Message text for users attempting to log on” is not set to the following, then this is a finding.

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC, monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

If the value for “Interactive Logon: Message title for users attempting to log on” is not set to “US DEPARTMENT OF DEFENSE WARNING STATEMENT” or its equivalent, then this is a finding.

Note: Any OS versions that do not support the full text version must state the following:

“I've read & consent to terms in IS user agreem't.”

Note: Deviations are not permitted except as authorized by the Deputy Assistant Secretary of Defense for Information and Identity Assurance.

Fix Text: Configure the system to display a logon banner that meets the DoD standards for a valid legal notice to users.

Group ID (Vulid): V-1090
Group Title: Caching of logon credentials
Rule ID: SV-28978r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.013
Rule Title: Caching of logon credentials is not limited.

Vulnerability Discussion: The default Windows configuration caches the last logon credentials for users who log on interactively to a system. This feature is provided for system availability reasons such as the users machine is disconnected from the network or domain controllers are not available. Even though the credential cache is well-protected, storing encrypted copies of users passwords on workstations do not always have the same physical protection required for domain controllers. If a workstation is attacked, the unauthorized individual may isolate the password to a domain user account using a password-cracking program, and gain access to the domain.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Interactive Logon: Number of previous logons to cache (in case Domain Controller is unavailable)” is not set to “2 logons” or less, then this is a finding.

Fix Text: Configure the system to save the credentials for 2 logons or less.

Group ID (Vulid): V-1091
Group Title: Halt on Audit Failure
Rule ID: SV-28980r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.015
Rule Title: System halts once an event log has reached its maximum size.

Vulnerability Discussion: This check verifies that the system will not halt if the audit logs become full.

Responsibility: System Administrator
IAControls: ECRR-1

Check Content:
FDCC XP and Vista - Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.

Navigate to Local Policies -> Security Options. If the value for “Audit: Shut down system immediately if unable to log security audits” is not set to “Disabled”, then this is a finding.

Fix Text: Configure the policy as specified in the manual check.

Group ID (Vulid): V-1093
Group Title: Restrict Anonymous Network Shares
Rule ID: SV-28982r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.018
Rule Title: Anonymous shares are not restricted.

Vulnerability Discussion: This is a Category 1 finding because it allows anonymous logon users (null session connections) to list all account names and enumerate all shared resources, thus providing a map of potential points to attack the system.

Documentable: YES
Potential Impacts:
In a mixed Windows environment this setting may cause systems with down-level operating systems to fail to authenticate, may prevent their users from changing their passwords, and may cause problems with managing printers and spools. In domains supporting Exchange 2003 servers and versions of Outlook earlier than Outlook 2003, the setting “Network access: Do not allow anonymous enumeration of SAM accounts and shares” should be set to “Disabled” on the Domain Controller Group Policy, to allow Outlook to anonymously query the global catalog service.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.

Navigate to Local Policies -> Security Options.
If the value for “Network access: Do not allow anonymous enumeration of SAM accounts” is not set to “Enabled”, then this is a finding.

If the value for “Network access: Do not allow anonymous enumeration of SAM accounts and shares” is not set to “Enabled”, then this is a finding.

Note: In domains supporting Exchange 2003 servers and versions of Outlook earlier than Outlook 2003, the setting “Network access: Do not allow anonymous enumeration of SAM accounts and shares” should be set to “Disabled” on the Domain Controller Group Policy, to allow Outlook to anonymously query the global catalog service.

Documentable Explanation: If the required settings cannot be used, in order to allow for proper operation in a mixed Windows environment, then this should be documented with the IAO. Exceptions to support the Exchange 2003 server and Outlook 2003 issue should also be documented with the IAO.

Fix Text: Configure the system to prevent anonymous users from listing account names and enumerating shared resources.

Group ID (Vulid): V-1097
Group Title: Bad Logon Attempts
Rule ID: SV-28986r1_rule

Severity: CAT II
Rule Version (STIG-ID): 4.002
Rule Title: Number of allowed bad-logon attempts does not meet minimum requirements.

Vulnerability Discussion: The account lockout feature, when enabled, prevents brute-force password attacks on the system. The higher this value is, the less effective the account lockout feature will be in protecting the local system. The number of bad logon attempts should be reasonably small to minimize the possibility of a successful password attack, while allowing for honest errors made during a normal user logon.

Responsibility: System Administrator
IAControls: ECLO-1, ECLO-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Account Policies -> Account Lockout Policy.

If the “Account lockout threshold” is "0" or more than three attempts, then this is a finding.

Fix Text: Configure the system to lock out an account after three invalid logon attempts.

Group ID (Vulid): V-1098
Group Title: Bad Logon Counter Reset
Rule ID: SV-29638r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.003
Rule Title: Time before bad-logon counter is reset does not meet minimum requirements.

Vulnerability Discussion: This parameter specifies the amount of time that must pass between two successive login attempts to ensure that a lockout will occur. The smaller this value is, the less effective the account lockout feature will be in protecting the local system.

Responsibility: System Administrator
IAControls: ECLO-1, ECLO-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Account Policies -> Account Lockout Policy.

If the “Reset account lockout counter after” value is less than 60 minutes, then this is a finding.

Fix Text: Configure the system to have the lockout counter reset itself after a minimum of 60 minutes.

Group ID (Vulid): V-1099
Group Title: Lockout Duration
Rule ID: SV-29642r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.004
Rule Title: Lockout duration does not meet minimum requirements.

Vulnerability Discussion: This parameter specifies the amount of time that must pass before a locked-out account is automatically unlocked by the system.

Responsibility: System Administrator
IAControls: ECLO-1, ECLO-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.

Expand the Security Configuration and Analysis tree view.
Navigate to Account Policies -> Account Lockout Policy.

If the “Account lockout duration” is not set to "0", requiring and administrator to unlock the account, then this is a finding.

Fix Text: Configure the system so that the bad logon lockout duration conforms to DoD requirements.

Group ID (Vulid): V-1102
Group Title: User Right - Act as part of OS
Rule ID: SV-28990r1_rule
Severity: CAT I
Rule Version (STIG-ID): 4.009
Rule Title: Unauthorized users are granted right to Act as part of the operating system.

Vulnerability Discussion: This is a Category 1 finding because users and user groups that are assigned this right can bypass all security protective mechanisms that apply to all users, including administrators. Accounts with this right should have passwords with the maximum length and be kept in a locked container accessible only by the IAO and his designated backup.

Some applications require this right to function. Any exception needs to be documented with the IAO.

Documentable: YES
Potential Impacts:
Removing application accounts from this right may cause the applications to stop functioning.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> User Rights Assignment.

If any user accounts, or groups (to include administrators),are granted the right "Act as part of the operating system", then this is a finding.

Documentable Explanation: Some applications require this right to function. Any exception needs to be documented with the IAO. Acceptable forms of documentation include vendor published documents and application owner confirmation.

Fix Text: Configure the system to prevent unauthorized users to "Act as part of the operating system".

Group ID (Vulid): V-1103
Group Title: User Rights Assignments
Rule ID: SV-18392r2_rule

Severity: CAT II
Rule Version (STIG-ID): 4.010
Rule Title: User rights and advanced user rights settings do not meet minimum requirements.

Vulnerability Discussion: Inappropriate granting of user and advanced user rights can provide system, administrative, and other high level capabilities not required by the normal user.

Documentable: YES
Potential Impacts:
Arbitrarily removing application accounts from certain User Rights may cause the applications to cease functioning.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Windows Vista

Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.

Navigate to Local Policies -> User Rights Assignment.

Compare the User Rights to the following list. if any unauthorized accounts are given rights that they are not authorized in the chart, then this is a finding.

Access this computer from network – Administrators

Act as part of the operating system – See separate vulnerability 4.009/V0001102

Adjust memory quotas for a process – Administrators, Local Service, Network Service

Allow logon locally – Administrators, Users

Allow logon through Terminal Services – (None)

Backup files and directories – Administrators

Bypass traverse checking – Administrators, Users, Local Service, Network Service

Change the system time – Administrators, Local Service

Change the time zone – Administrators, Users, Local Service

Create a pagefile – Administrators

Create a token object – (None)

Create global objects – Administrators, Service, Local Service, Network Service

Create permanent shared objects – (None)

Create symbolic links – Administrators

Debug programs – See separate vulnerability 4.005/V0018010

Deny access to this computer from the network – See separate vulnerability 4.025/V0001155

Deny logon as a batch job – Guests

Deny logon as a service – (None)

Deny logon locally – Guests

Deny logon through Terminal Services – Everyone (Guests if TS is used)

Enable computer and user accounts to be trusted for delegation – (None)

Force shutdown from a remote system – Administrators

Generate security audits – Local Service, Network Service

Impersonate a client after authentication – Administrators, Service, Local Service, Network Service

Increase a process working set – Administrators, Local Service

Increase scheduling priority – Administrators

Load and unload device drivers – Administrators

Lock pages in memory – (None)

Log on as a batch job – (None)

Log on as a service – (None)

Manage auditing and security log – "Auditor's" Group

Modify an object label – (None)

Modify firmware environment values – Administrators

Perform volume maintenance tasks – Administrators

Profile single process – Administrators

Profile system performance – Administrators

Remove computer from docking station – Administrators, Users

Replace a process level token – Local Service, Network Service

Restore files and directories – Administrators

Shut down the system – Administrators, Users

Take ownership of files or other objects – Administrators

Documentable Explanation: Some applications require one or more of these rights to function. Any exception needs to be documented with the IAO. Acceptable forms of documentation include vendor published documents and application owner confirmation.

Fix Text: Configure the system to prevent accounts from having unauthorized User Rights.

Group ID (Vulid): V-1104
Group Title: Maximum Password Age
Rule ID: SV-29646r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.011
Rule Title: Maximum password age does not meet minimum requirements.

Vulnerability Discussion: The longer a password is in use, the greater the opportunity for someone to gain unauthorized knowledge of the passwords. Further, scheduled changing of passwords hinders the ability of unauthorized system users to crack passwords and gain access to a system.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Account Policies -> Password Policy.

If the value for the “Maximum password age” is greater than 60 days, then this is a finding. If the value is set to 0 (never expires), then this is a finding.

Fix Text: Configure the Maximum Password Age so that it is not "0" and doesn't exceed 60 days.

Group ID (Vulid): V-1105
Group Title: Minimum Password Age
Rule ID: SV-28994r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.012
Rule Title: Minimum password age does not meet minimum requirements.

Vulnerability Discussion: Permitting passwords to be changed in immediate succession within the same day, allows users to cycle passwords through their history database. This enables users to effectively negate the purpose of mandating periodic password changes.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Account Policies -> Password Policy.

If the value for the “Minimum password age” is less than one day, then this is a finding.

Fix Text: Configure the Minimum Password Age so that it is a minimum of "1".

Group ID (Vulid): V-1107
Group Title: Password Uniqueness
Rule ID: SV-29651r1_rule

Severity: CAT II
Rule Version (STIG-ID): 4.014
Rule Title: Password uniqueness does not meet minimum requirements.

Vulnerability Discussion: A system is more vulnerable to unauthorized access when system users recycle the same password several times without being required to change a password to a unique password on a regularly scheduled basis. This enables users to effectively negate the purpose of mandating periodic password changes.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Account Policies -> Password Policy.

If the value for “Enforce password history” is less than 24 passwords, then this is a finding.

Fix Text: Configure the system to remember a minimum of "24" used passwords.

Group ID (Vulid): V-1112
Group Title: Dormant Accounts
Rule ID: SV-29481r1_rule
Severity: CAT III
Rule Version (STIG-ID): 4.019
Rule Title: User account is dormant.

Vulnerability Discussion: Outdated or unused accounts, provide penetration points that may go undetected.

False Positives:
The reviewer should review the list with the SA to determine the finding validity for each account reported.

Documentable: YES
Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
Using the DUMPSEC utility:

Select “Dump Users as Table” from the “Report” menu.
Select the available fields in the following sequence, and click on the “Add” button for each entry:
UserName
SID
PswdRequired
PswdExpires
PswdLastSetTime
LastLogonTime
AcctDisabled
Groups

If any enabled accounts have not been logged into within the past 35 days, then this is a finding. This can be ascertained by examining the time in the “LastLogonTime” column. The following accounts are exempt from this check:

The built-in administrator account
The built-in guest account

Application accounts
The “IUSR”-guest account (used with IIS or Peer Web Services)
Accounts that are less than 35 days old
Disabled accounts

Note: The reviewer should review the list with the SA to determine the finding validity for each account reported.

Note: The following command can be used on Windows 2003/2008 Active Directory if DumpSec cannot be run:

Open a Command Prompt
Enter “Dsquery user -limit 0 -inactive 5 -o rdn” (This command will only work if the domain is at least at a Windows Server 2003 functional level, not Windows 2000 Native).
A list of user accounts that have been inactive for 5 weeks will be displayed.

Disabled Accounts can be determined by using the following:
Enter “Dsquery user -limit 0 -disabled -o rdn”.

Documentable Explanation: Dormant accounts that have been reviewed and deemed to be required should be documented with the IAO.

Fix Text: Regularly review accounts to determine if they are still active. Accounts that have not been used in the last 35 days should either be removed or disabled.

Group ID (Vulid): V-1113
Group Title: Disable Guest Account
Rule ID: SV-29656r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.020
Rule Title: The built-in guest account is not disabled.

Vulnerability Discussion: A system faces an increased vulnerability threat if the built-in guest account is not disabled. This account is a known account that exists on all Windows systems and cannot be deleted. This account is initialized during the installation of the operating system with no password assigned. This account is a member of the Everyone user group and has all the rights and permissions associated with that group, which could subsequently provide access to system resources to anonymous users.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Accounts: Guest account status” is not set to ” Disabled”, then this is a finding.

Fix Text: Configure the system to disable the built-in guest Account.

Group ID (Vulid): V-1114
Group Title: Rename Built-in Guest Account
Rule ID: SV-29484r1_rule

Severity: CAT II
Rule Version (STIG-ID): 4.021
Rule Title: The built-in guest account has not been renamed.

Vulnerability Discussion: A system faces an increased vulnerability threat if the built-in guest account is not renamed or disabled. The built-in guest account is a known user account on all Windows systems, and as initially installed, does not require a password. This can allow access to system resources by unauthorized users. This account is a member of the group Everyone and has all the rights and permissions associated with that group and could provide access to system resources to unauthorized users.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Accounts: Rename guest account” is not set to a value other than “Guest”, then this is a finding.

Fix Text: Configure the system to rename the built-in guest account

---

Group ID (Vulid): V-1115
Group Title: Rename Built-in Administrator Account
Rule ID: SV-28997r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.022
Rule Title: The built-in administrator account has not been renamed.

Vulnerability Discussion: The built-in administrator account is a well known account. Renaming the account to an unidentified name improves the protection of this account and the system.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Accounts: Rename administrator account” is not set to a value other than “Administrator”, then this is a finding.

Fix Text: Configure the system to rename the built-in administrator account.

Group ID (Vulid): V-1118
Group Title: Event Log Sizes
Rule ID: SV-16946r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.002
Rule Title: Event log sizes do not meet minimum requirements.

Vulnerability Discussion: Inadequate log size will cause the log to fill up quickly and require frequent clearing by administrative personnel.

Documentable: YES
Potential Impacts:
Microsoft recommends that the combined size of all the event logs (including DNS logs, Directory Services logs, and Replication logs on Servers or Domain Controllers) should not exceed 300 megabytes. Exceeding the recommended value can impact performance.

Responsibility: System Administrator
IAControls: ECRR-1

Check Content:
Vista/2008 - If the following registry values don't exist or are not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE

Subkey: Software\Policies\Microsoft\Windows\EventLog\Application
Value Name: MaxSize
Type: REG_DWORD
Value: 32768

Subkey: Software\Policies\Microsoft\Windows\EventLog\Security
Value Name: MaxSize
Type: REG_DWORD
Value: 81920

Subkey: Software\Policies\Microsoft\Windows\EventLog\Setup
Value Name: MaxSize
Type: REG_DWORD
Value: 32768

Subkey: Software\Policies\Microsoft\Windows\EventLog\System
Value Name: MaxSize
Type: REG_DWORD
Value: 32768

Documentable: Yes
Documentable Explanation: If the machine is configured to write an event log directly to an audit server, the "Maximum log size" for that log does not have to conform to the requirements above. This should be documented with the IAO.

Fix Text: Configure the following policy values as listed below:

Computer Configuration -> Administrative Templates -> Windows Components -> Event Log Service ->

Application -> "Maximum Log Size (KB)" will be set to "Enabled:32768"
Security -> "Maximum Log Size (KB)" will be set to "Enabled:81920"
Setup -> "Maximum Log Size (KB)" will be set to "Enabled:32768"
System -> "Maximum Log Size (KB)" will be set to "Enabled:32768"

Group ID (Vulid): V-1119
Group Title: Booting into Multiple Operating Systems
Rule ID: SV-19250r3_rule

Severity: CAT II
Rule Version (STIG-ID): 5.003
Rule Title: Booting into alternate operating systems is permitted.

Vulnerability Discussion: Allowing other operating systems to run on a secure system, can allow users to circumvent security. If more than one operating system is installed on a computer, each must be configured to be compliant with STIG guidance.

False Positives:
Review each alternate OS boot option with the SA.

Potential Impacts:
The system is not configured to prevent booting into non-compliant alternate operating systems.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open the Control Panel
Double-click on the “System” applet.
Click on the “Advanced System Settings” link.
Click on the “Advanced” tab.
Click the Startup and Recovery “Settings” button.

If the drop-down listbox in System Startup shows any operating system other than the current Windows OS, this may be a finding. If all additional operating systems are STIG compliant, then this is not a finding.

Fix Text: Configure the system to prevent running non-compliant alternate operating systems.

Group ID (Vulid): V-1120
Group Title: Prohibited FTP Logins
Rule ID: SV-29492r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.004
Rule Title: Installed FTP server is configured to allow prohibited logins.

Vulnerability Discussion: The FTP (File Transfer Protocol) service allows remote users to access shared files and directories. Allowing anonymous FTP makes user auditing difficult.

Using accounts that have administrator privileges to log on to FTP risks that the user id and password will be captured on the network, and give administrator access to an unauthorized user.

Security Override Guidance:
If accounts with administrator privileges are used to access FTP, then this becomes a Category I finding.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
In the “Command Prompt” window, enter the following command, and attempt to logon as the user “anonymous:”

C:\>ftp 127.0.0.1
(Connected to ftru014538.ncr.disa.mil.
220 ftru014538 Microsoft FTP Service (Version 2.0).)

User: anonymous

(331 Anonymous access allowed, send identity (e-mail name) as password.)

Password: password
(230 Anonymous user logged in.)
ftp>

If the command response indicates that an anonymous FTP login was permitted, then this is a finding.

Severity Override: If accounts with administrator privileges are used to access FTP, then this becomes a Category I finding.

Fix Text: Configure the system to prevent an installed FTP service from allowing prohibited logons.

Group ID (Vulid): V-1121
Group Title: FTP System File Access
Rule ID: SV-29496r1_rule
Severity: CAT I
Rule Version (STIG-ID): 5.005
Rule Title: Installed FTP server is configured to allow access to the system drive.

Vulnerability Discussion: This is a Category 1 finding because the FTP service allows remote users to access shared files and directories which could provide access to system resources and compromise the system, especially if the user can gain access to the root directory of the boot drive.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
In the "Command Prompt" window, enter the following command, log on using an authenticated FTP account, and attempt to access the root of the boot drive:

X:\>ftp 127.0.0.1
(Connected to ftru065103.ncr.disa.mil.
220 ftru065103 Microsoft FTP Service (Version 2.0).)

User: ftpuser
(331 Password required for ftpuser.)

Password: password
(230 User ftpuser logged in.)

ftp> dir /

If the FTP session indicates access to operating system files like "PAGEFILE.SYS" or "NTLDR," then this is a finding.

Fix Text: Configure the system to prevent an FTP Service from allowing access to the system drive.

Group ID (Vulid): V-1122
Group Title: Password Protected Screen Saver

Rule ID: SV-29500r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.006
Rule Title: The system configuration is not set with a password-protected screen saver.

Vulnerability Discussion: The system should be locked when unattended. Unattended systems are susceptible to unauthorized use. The screen saver should be set at a maximum of 15 minutes and password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer.

Documentable: YES
Responsibility: System Administrator
IAControls: PESL-1

Check Content:
If the any of the registry values don't exist or are not configured as follows, then this is a finding:

Registry Hive: HKEY_CURRENT_USER
Subkey: \Software\Policies\Microsoft\Windows\Control Panel\Desktop\

Value Name: ScreenSaveActive
Type: REG_SZ
Value: 1

Value Name: ScreenSaverIsSecure
Type: REG_SZ
Value: 1

Value Name: ScreenSaveTimeOut
Type: REG_SZ
Value: 900 (or less)

Documentable Explanation: Terminal servers and applications requiring continuous, real-time screen display (i.e., network management products) require the following and need to be documented with the IAO.

-The logon session does not have administrator rights.
-The display station (i.e., keyboard, monitor, etc.) is located in a controlled access area.

Fix Text: Configure The policy values for User Configuration -> Administrative Templates -> Control Panel -> Display as follows:

"Screen Saver" will be set to "Enabled" ("Activate screen saver" on Windows 2000)

"Password protect the screen saver" will be set to "Enabled"

"Screen Saver timeout" will be set to "Enabled: 900 seconds" (or less)

Group ID (Vulid): V-1127
Group Title: Restricted Administrator Group Membership
Rule ID: SV-29504r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.027
Rule Title: A non-administror account has Administrator rights on the system.

Vulnerability Discussion: An account who does not have administrator duties should not have Administrator rights. Such rights would allow the account to bypass or modify required security restrictions on that machine and make it vulnerable to attack from both internal and external sources.

False Positives:
The reviewer should review all questionable accounts with the SA.

Documentable: YES
Responsibility: System Administrator
IAControls: ECPA-1

Check Content:
If an account, without administrator duties, is a member of the Administrators group, then this is a finding.

Note: The Gold Disk will return a list of all accounts in Administrator groups for review to determine applicability.

Using the DUMPSEC utility:

Select “Dump Users as Table” from the “Report” menu.
Select the available fields in the following sequence, and click on the “Add” button for each entry:
UserName
SID
PswdRequired
PswdExpires
LastLogonTime
AcctDisabled
Groups

Documentable Explanation: Approved exceptions to this requirement should be documented with the IAO.

Fix Text: Configure the system to prevent non-administrators from having administrator rights.

Group ID (Vulid): V-1128
Group Title: Security Configuration Tools
Rule ID: SV-29668r1_rule
Severity: CAT III
Rule Version (STIG-ID): 1.016
Rule Title: Security Configuration Tools are not being used to configure platforms for security compliance.

Vulnerability Discussion: Security Configuration tools such as Security Templates and Group Policy allow system administrators to consolidate all security related system settings into a single configuration file. These settings can then be applied consistently to any number of Windows Machines. The Security Configuration tools can use the same configuration file to check platforms for compliance with security policy.

False Positives:
If an alternate method is used to configure a system (e.g. Gold Disk, manually - using the DISA Windows Security Checklist), that achieves the same configured result, then this is acceptable.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Interview the SA to determine if the Security Configuration tools, or equivalent process, is being used to configure Windows systems to meet security requirements. The Microsoft Security Configuration tools (such as Security Templates and Group Policy that are integrated into Windows) should be used to configure platforms for security compliance.

Note: If an alternate method is used to configure a system (e.g. Gold Disk, manually - using the DISA Windows Security Checklist, etc.) that achieves the same configured result, then this is acceptable.

Fix Text: Security Configuration tools or equivalent should be used to configure Windows systems to meet security requirements.

Group ID (Vulid): V-1130
Group Title: System File ACLs
Rule ID: SV-16968r2_rule
Severity: CAT II
Rule Version (STIG-ID): 2.006
Rule Title: ACLs for system files and directories do not conform to minimum requirements.

Vulnerability Discussion: Failure to properly configure ACL file and directory permissions, allows the possibility of unauthorized and anonymous modification to the operating system and installed applications.

False Positives:
If a manual check of a questionable ACL setting shows that it has been set to meet or is more restrictive than minimum requirements, then it will not be counted as a finding.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
The default ACL settings are adequate when the Security Option “Network access: Let everyone permissions apply to anonymous users” is set to “Disabled” and Power User Group Membership is restricted.

If the option is set to “Disabled” and Powers Users are restricted, this check should normally be marked “Not a Finding”

Note: Additional ACL requirements may be listed in Appendix A.

Note: Power Users is included in Server 2008 for backward compatibility.

Note: If an ACL setting prevents a site’s applications from performing properly, the site can modify that specific setting. Settings should only be changed to the minimum necessary for the application to function. Each exception to the recommended settings should be documented and kept on file by the IAO.

Fix Text: Vista/2008/7 - Configure the Security Option:

“Network access: Let everyone permissions apply to anonymous users” to “Disabled”

and

Restrict the Power Users group to include no memebers.

Group ID (Vulid): V-1131
Group Title: Strong Password Filtering
Rule ID: SV-29673r1_rule

Severity: CAT II
Rule Version (STIG-ID): 2.009
Rule Title: A password filter that enforces DoD requirements is not installed.

Vulnerability Discussion: Password complexity software (ie. PPEc32.dll for DISANET and some Services), when installed properly, places restrictions on how new passwords are defined through the Control-Alt-Delete dialog. The following policy is implemented:

* Passwords must contain 1 characters from the following 4 classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Sites are responsible for installing password complexity software that complies with current DOD requirements.

Security Override Guidance:
If no password filter is used, and the security option for "Password must meet complexity requirements" (V0001150/3.028) is set to "Enabled", then this finding can be downgraded to a Category III, since a less strict complexity algorithm is used.

Responsibility: System Administrator
IAControls: IAIA-1

Check Content:
Password complexity is a case-sensitive character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each.

This check determines whether the site has implemented a password filter that enforces the DoD requirements listed above.

The enpasflt.dll password filter can be found on Gold Disk CD1 in the Install\Misc directory. It should be tested for the particular environment and may be used on Windows versions the Gold Disk does not currently support. The Date Modified should be 1/6/2000.

For the enpasflt.dll password filter to function properly:

•Copy enpasflt.dll file into %systemroot%\system32
•Registry key "HKLM\System\CurrentControlSet\Control\LSA\Notification Packages" must include "enpasflt"
•Restart the system

If the enpasflt.dll password filter does not function properly or causes issues in a particular environment, the site will be responsible for obtaining another password filter to meet the requirements.

If PPE or another product is used, then the reviewer should have the SA show that it is configured to enforce the DoD requirements.

Severity Override: If no password filter is used, and the security option for "Password must meet complexity requirements" (V0001150/3.028) is set to "Enabled", then this finding can be downgraded to a Category III, since a less strict complexity algorithm is used.

Note: If a password filter is not used, the site is still responsible for requiring full compliance with DoD policy, even though the password complexity setting does not enforce the 4-character type rule.

Fix Text: Install a password filter and configure it to function properly and enforce the required DoD standards.

Group ID (Vulid): V-1135

Group Title: Printer Share Permissions
Rule ID: SV-29510r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.027
Rule Title: Printer share permissions are not configured as recommended.

Vulnerability Discussion: Improperly configured share permissions on printers can permit the addition of unauthorized print devices on the network. Windows shares are a means by which files, folders, printers, and other resources can be published for network users to remotely access. Regular users cannot create shares on their local machines; only Administrators and Power Users have that ability.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
Run Windows Explorer.
Select the Control Panel folder. (NT=Printers folder)
Select the Printers folder.

If there are no locally attached printers, then mark this as “Not Applicable.”

Perform this check for each locally attached printer:

Right click on a locally-attached printer.
Select Sharing from the drop-down menu.

Perform this check on each printer that has the “Shared” radio-button selected:

Select the Security tab

The following table lists the recommended printer share security settings (Allow Permission):

Users - Print
Administrators, System, Creator Owner - Print, Manage Printers, Manage Documents

If there are no shared local printers, then mark this as “Not Applicable.”
If the share permissions do not match the above table, then this is a finding.

Fix Text: Configure the permissions on locally shared printers to meet the minimum requirements.

Group ID (Vulid): V-1136
Group Title: Forcibly Disconnect when Logon Hours Expire
Rule ID: SV-29000r1_rule
Severity: CAT III
Rule Version (STIG-ID): 4.006
Rule Title: Users are not forcibly disconnected when logon hours expire.

Vulnerability Discussion: Users should not be permitted to remain logged on to the network after they have exceeded their permitted logon hours. In many cases, this indicates that a user forgot to log off before leaving for the day. However, it may also indicate that a user is attempting unauthorized access at a time when the system may be less closely monitored. This protects critical and sensitive network data from exposure to unauthorized personnel with physical access to the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Microsoft Network Server: Disconnect Clients When Logon Hours Expire” is not set to “Enabled”, then this is a finding.

Note: The Gold Disk uses an API call to check internal system values, in addition to checking the related registry setting for this value. Using the MMC to review this setting may return a false negative; therefore, the Gold Disk result takes precedence. Setting this value with either the Gold Disk or the MMC updates the internal values as well as the appropriate registry
value.

Fix Text: Configure the system to forcibly disconnect users when logon hours expire.

Group ID (Vulid): V-1137
Group Title: Access Restrictions to Logs
Rule ID: SV-29778r1_rule
Severity: CAT II
Rule Version (STIG-ID): 1.010
Rule Title: An Auditors group has not been created to restrict access to the Windows Event Logs.

Vulnerability Discussion: The Security Event Log contains information on security exceptions that occur on the system. This data is critical for identifying security vulnerabilities and intrusions. The Application and System logs can also contain information that is critical in assessing security events. Therefore, these logs must be protected from unauthorized access and modification.

An Auditors group will be used to restrict access to auditing through the User Right “Manage auditing and security log” (V-1103) and for assigning permissions to event logs (V-1077).

Only individuals who have auditing responsibilities (IAO, IAM, auditors, etc.) should be members of this group.

The individual System Administrators responsible for maintaining this system can also be members of this group.

Responsibility: System Administrator
IAControls: ECTP-1

Check Content:
Interview the SA to determine if an Auditors group for controlling the Windows Event Logs has been created.

NOTE: The administrator(s) responsible for the installation and maintenance of the individual system(s) must be a member(s) of the Auditors group. This will permit the responsible administrator to enable and configure system auditing, and perform maintenance functions related to the logs. Administrators who are not responsible for maintenance on an individual system will not be included in the Auditors group.

Fix Text: Create an Auditors group for controlling the Windows Event Logs and assign the necessary rights and access controls.

Group ID (Vulid): V-1140
Group Title: Users with Administrative Privilege
Rule ID: SV-29680r1_rule
Severity: CAT II
Rule Version (STIG-ID): 1.006
Rule Title: Users with Administrative privilege are not documented or do not have separate accounts for administrative duties and normal operational tasks.

Vulnerability Discussion: Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges.

The rule of least privilege should always be enforced.

Responsibility: Information Assurance Officer
IAControls: ECLP-1

Check Content:
Ask the System Administrator (SA) to show the necessary documentation that identifies the members of this privileged group.

This check verifies that each user with administrative privileges has been assigned a unique account, separate from the built-in "Administrator" account. This check also verifies that the default "Administrator" account is not being used. Administrators should be properly trained before being permitted to perform administrator duties. The IAO will maintain a list of all users belonging to the Administrator's group.

If any of the following conditions are true, then this is a finding:

•Each SA does not have a unique userid dedicated for administering the system.
•Each SA does not have a separate account for normal user tasks.
•The built-in administrator account is used to administer the system.
•Administrators have not been properly trained.
•The IAO does not maintain a list of users belonging to the Administrator's group.

Fix Text: Create the necessary documentation that identifies the members of this privileged group. Ensure that each member has a separate account for user duties and one for his privileged duties and the other requirements outlined in the manual check are met.

Group ID (Vulid): V-1141
Group Title: Unencrypted Password is Sent to SMB Server.
Rule ID: SV-29003r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.034
Rule Title: Unencrypted password is sent to 3rd party SMB Server.

Vulnerability Discussion: Some non-Microsoft SMB servers only support unencrypted (plain text) password authentication. Sending plain text passwords across the network, when authenticating to an SMB server, reduces the overall security of the environment. Check with the Vendor of the SMB server to see if there is a way to support encrypted password authentication.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.

Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Microsoft Network Client: Send unencrypted password to connect to third-party SMB servers” is not set to “Disabled”, then this is a finding.

Fix Text: Configure the system to prevent unencrypted passwords from being sent to third-party SMB servers.

Group ID (Vulid): V-1145
Group Title: Disable Administrator Automatic Logon
Rule ID: SV-29006r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.040
Rule Title: Administrator automatic logon is enabled.

Vulnerability Discussion: This is a category 1 finding because it will directly log on to the system with administrator privileges when the machine is rebooted. This would give full access to any unauthorized individual who reboots the computer.

By default this setting is not enabled. If this setting exists, it should be disabled. If this capability exists, the password may also be present in the registry, and must be removed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.

Navigate to Local Policies -> Security Options.
If the value for “MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)” is not set to “Disabled”, then this is a finding.

The policy referenced above will update the following registry value:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows NT\CurrentVersion\Winlogon\

Value Name: AutoAdminLogon
Type: REG_SZ
Value: 0

Note: The Gold Disk will also check for the existence of the HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\defaultpassword value. If it exists this will also make this a finding.

Fix Text: Configure the system to disable automatic administrator logon.

Group ID (Vulid): V-1148
Group Title: Local Users Exist on a Workstation
Rule ID: SV-29512r1_rule
Severity: CAT III
Rule Version (STIG-ID): 4.024
Rule Title: Local users exist on a workstation in a domain.

Vulnerability Discussion: To minimize potential points of attack, local users, other than built-in accounts such as Administrator and Guest accounts, should not exist on a workstation in a domain. Users should always log onto workstations in a domain domain with their domain accounts. This does not apply to laptop PCs which are designed to function both on the domain and off the domain.

False Positives:
This does not apply to laptops that are designed to function both as part of a domain and separate from it.

Documentable: YES
Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
If local users other than the built-in accounts listed below exist on a workstation in a domain this is a finding.

Built-in Administrator (renamed)
Built-in Guest (renamed)
HelpAssistant (XP only)
Support_388945a0 (XP only)

The Gold Disk will return a list of local accounts for review to determine applicability.

Note: This does not apply to laptops that are designed to function both as part of a domain and separate from it.

Using the DUMPSEC utility:

Select “Dump Users as Table” from the “Report” menu.
Select the available fields in the following sequence, and click on the “Add” button for each entry:
UserName
SID
PswdRequired
PswdExpires
LastLogonTime
AcctDisabled
Groups

Documentable Explanation: If a site has need of special purpose local user accounts, then this should be documented with the IAO.

Fix Text: Configure the system to restrict the existence of local user accounts.

Group ID (Vulid): V-1150
Group Title: Microsoft Strong Password Filtering
Rule ID: SV-29684r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.028
Rule Title: The built-in Microsoft password filter is not enabled.

Vulnerability Discussion: This policy setting configures the local system to verify that newly-created passwords conform to the more stricter policy.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Account Policies -> Password Policy.

If the value for “Password must meet complexity requirements” is not enabled, then this is a finding.

Note: If the site is using a password filter that requires this setting be set to “Disabled” for the filter code to be used, then this would not be considered a finding.

Note: DISANET and some DoD sites require the use of Password Policy Enforcer (PPE). This setting has no effect on the use of PPE when it is installed. However, it will be enabled for fall-back purposes.

Fix Text: Configure the system to enable filtering for complex passwords.

Group ID (Vulid): V-1151
Group Title: Secure Print Driver Installation
Rule ID: SV-29009r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.029
Rule Title: Print driver installation privilege is not restricted to administrators.

Vulnerability Discussion: By default, the print spooler allows any user to add and to delete printer drivers on the local system. This capability should be restricted to the Administrators user group, the Print Operators user group on server platforms.

Documentable: YES
Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Devices: Prevent users from installing printer drivers” is not set to “Enabled”, then this is a finding.

Documentable Explanation: If site circumstances require that users be able to install print drivers for locally attached printers (e.g. - Users that telecommute and attach a home printer), this exception can be documented with the site IAO.

Fix Text: Configure the system to restrict the installation of print drivers to only authorized groups.

Group ID (Vulid): V-1152
Group Title: Anonymous Access to the Registry
Rule ID: SV-29594r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.030
Rule Title: Anonymous access to the Registry is not restricted.

Vulnerability Discussion: This is a Category I finding, because this vulnerability allows an anonymous individual read-access and write-access to some parts of the Registry.

The permissions set for the Winreg subkey determine who can remotely connect to a registry. If this subkey does not exist, all users can remotely connect to the registry. To remotely connect to a registry, a user must have at least Read Access to the Winreg subkey on the target computer.

The Everyone group, which is given permissions by the default installation, typically has at least enough access allowed to browse. Therefore, the capability for an anonymous user to access the Registry over the network must be prevented.

Documentable: YES
Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Wiindows XP/2003/Vista/2008 - Using the Registry Editor, navigate to the following Key: MACHINE/System/CurrentControlSet/Control/SecurePipeServers/Winreg If the key does not exist, then this is a finding. If the permissions are not at least as restrictive as those below, then this is a finding. Administrators all Backup Operators read(QENR) Local Service read (Exchange Enterprise Servers group on Domain Controllers and Exchange server all

Documentable Explanation: On DCs and Exchange Servers, if permissions are sub-delegated with the Exchange Management console, then additional accounts and groups may appear on the Winreg key. If this has been done then these should be documented with the site IAO and made available for any reviewer.

Fix Text: Configure the system to prevent anonymous users from gaining access to the Registry.

Group ID (Vulid): V-1153
Group Title: LanMan Authentication Level
Rule ID: SV-29012r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.031
Rule Title: The Send download LanMan compatible password option is not set to Send NTLMv2 response only\refuse LM.

Vulnerability Discussion: The Kerberos v5 authentication protocol is the default for authentication of users who are logging on to domain accounts from computers that are running Windows 2000 or later. The Kerberos protocol is the protocol of choice since Windows 2000, when there is a choice.

NTLM is retained in later Windows versions for compatibility with clients and servers that are running earlier versions of Windows. It is also used to authenticate logons to stand-alone computers that are running later versions.

Documentable: YES
Potential Impacts:
Setting this to the required setting may prevent authentication with older Operating Systems and break some applications.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Network security: LAN Manager authentication level” is not set to at least “Send NTLMv2

response only\refuse LM" (Level 4), then this is a finding.

Documentable Explanation: In a mixed Windows environment, if this setting needs to be loosened due to compatibility issues, then the reasons need to be documented with the IAO.

Fix Text: Configure the system to the required level of LanMan authentication.

Group ID (Vulid): V-1154
Group Title: Ctrl+Alt+Del Security Attention Sequence
Rule ID: SV-29015r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.032
Rule Title: Ctrl+Alt+Del security attention sequence is Disabled.

Vulnerability Discussion: Disabling the Ctrl+Alt+Del security attention sequence can compromise system security. Because only Windows responds to the Ctrl+Alt+Del security sequence, you can be assured that any passwords you enter following that sequence are sent only to Windows. If you eliminate the sequence requirement, malicious programs can request and receive your Windows password. Disabling this sequence also suppresses a custom logon banner.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for "Interactive Logon: Do not require CTRL+ALT+DEL" is not set to "Disabled", then this is a finding.

Fix Text: Configure the system to require the Ctrl+Alt+Del key sequence to log on.

Group ID (Vulid): V-1155
Group Title: Deny Access from the Network
Rule ID: SV-29598r1_rule
Severity: CAT I
Rule Version (STIG-ID): 4.025
Rule Title: User Right to Deny Access to this computer from the network is not configured to include Guests. (Anonymous Logon and Support_388945a0 in applicable Windows versions).

Vulnerability Discussion: This is a Category 1 finding because allowing network logins by the built-in guest accounts, which are a member of the Everyone group and Guests group, with all the rights and permissions associated with that group, could provide anonymous access to system resources to unauthorized users. Anonymous Logon and Support_388945a0 are also included in applicable Windows versions.

Documentable: YES
Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.

Navigate to Local Policies -> User Rights Administration.

If the following groups/accounts are not listed under the right "Deny access to this computer from the network", then this is a finding.

Windows 2000 - Guests

Windows 2003 - Guests, Anonymous Logon, Support_388945a0

Windows XP - Guests, Support_388945a0

Vista - Guests

Windows 2008 - Guests

Note: If an account listed has been deleted from the system such as the Support_388945a0 account, the Gold Disk may incorrectly report the account as a finding. If the account does not exist on a system it would not be a finding.

Documentable Explanation: On Exchange Server 2003 supporting OWA, the Guests group should be removed and replaced with “Anonymous Logon”. Document with the IAO

Fix Text: Configure the system to give the right "Deny access to this computer from the network" to the Accounts/Groups specified in the manual check.

Group ID (Vulid): V-1157
Group Title: Smart Card Removal Option
Rule ID: SV-28467r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.047
Rule Title: The Smart Card removal option is set to take no action.

Vulnerability Discussion: Determines what should happen when the smart card for a logged-on user is removed from the smart card reader.

The options are:
- No Action
- Lock Workstation
- Force Logoff

Documentable: YES
Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.

Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options.

If the value for “Interactive logon: Smart card removal behavior” is not set to “Lock Workstation”, or “Force Logoff”, then this is a finding.

Documentable Explanation: This can be left not configured or set to “No action” on workstations with the following conditions. This will be documented with the IAO.
•The setting can't be configured due to mission needs, interferes with applications.
•Policy must be in place that users manually lock workstations when leaving them unattended.

•Screen saver requirement is properly configured to lock as required in V0001122.

Fix Text: Configure the system to, at a minimum, lock the system if a smart card is removed.

Group ID (Vulid): V-1158
Group Title: Recovery Console - SET Command
Rule ID: SV-29019r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.048
Rule Title: The Recovery Console SET command is enabled.

Vulnerability Discussion: Enabling this option enables the Recovery Console SET command, which allows you to set Recovery Console environment variables. This permits floppy copy and access to all drives and folders.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Recovery Console: Allow floppy copy and access to all drives and folders” is not set to “Disabled”, then this is a finding.

Fix Text: Configure the system to disable the Recovery Console ability to do floppy copy and have access to all drives.

Group ID (Vulid): V-1159
Group Title: Recovery Console - Automatic Logon
Rule ID: SV-29023r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.049
Rule Title: The Recovery Console option is set to permit automatic logon to the system.

Vulnerability Discussion: This is a Category 1 finding because if this option is set, the Recovery Console does not require you to provide a password and will automatically log on to the system, giving Administrator access to system files.

By default, the Recovery Console requires you to provide the password for the Administrator account before accessing the system.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Recovery Console: Allow automatic administrative logon” is not set to “Disabled”, then this is a finding.

Fix Text: Configure the system to prevent the Recovery Console from automatically logging on.

Group ID (Vulid): V-1162
Group Title: SMB Server Packet Signing (if client agrees)
Rule ID: SV-29026r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.046
Rule Title: The Windows SMB server is not enabled to perform SMB packet signing when possible.

Vulnerability Discussion: If this policy is enabled, it causes the Windows Server Message Block (SMB) server to perform SMB packet signing.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Microsoft Network Server: Digitally sign communications (if client agrees)” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to have the SMB server sign SMB packets when possible.

Group ID (Vulid): V-1163
Group Title: Encryption of Secure Channel Traffic
Rule ID: SV-29514r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.043
Rule Title: Outgoing secure channel traffic is not encrypted when possible.

Vulnerability Discussion: Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but not all information is encrypted. If this policy is enabled, outgoing secure channel traffic should be encrypted.

False Positives:
If the value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”, then this would not be a finding.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Domain Member: Digitally encrypt secure channel data (when possible)” is not set to “Enabled”, then this is a finding.

Note: If the value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”, then this would not be a finding.

Fix Text: Configure the system to encrypt outgoing secure traffic when possible.

Group ID (Vulid): V-1164
Group Title: Signing of Secure Channel Traffic
Rule ID: SV-29517r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.042
Rule Title: Outgoing secure channel traffic is not signed when possible.

Vulnerability Discussion: Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked. If this policy is enabled, all outgoing secure channel traffic should be signed.

False Positives:
If the value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”, then this would not be a finding.

Responsibility: System Administrator
IAControls: DCNR-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Domain Member: Digitally sign secure channel data (when possible)” is not set to “Enabled”, then this is a finding.

Note: If the value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”, then this would not be a finding.

Fix Text: Configure the system to sign SMB traffic when possible.

Group ID (Vulid): V-1165
Group Title: Computer Account Password Reset
Rule ID: SV-29029r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.044
Rule Title: The computer account password is prevented from being reset.

Vulnerability Discussion: As a part of Windows security, computer account passwords are changed automatically. Enabling this policy to disable automatic password changes can make the system more vulnerable to malicious access. Frequent password changes can be a significant safeguard for your system. If this policy is disabled, a new password for the computer account will be generated every week.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.

Expand the Security Configuration and Analysis tree view.

Navigate to Local Policies -> Security Options.
If the value for “Domain Member: Disable Machine Account Password Changes” is not set to “Disabled”, then this is a finding.

Fix Text: Configure the system to permit the computer account password to be changed.

Group ID (Vulid): V-1166
Group Title: SMB Client Packet Signing (if server agrees)
Rule ID: SV-29032r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.045
Rule Title: The Windows SMB client is not enabled to perform SMB packet signing when possible.

Vulnerability Discussion: If this policy is enabled, it causes the Windows Server Message Block (SMB) client to perform SMB packet signing when communicating with an SMB server that is enabled or required to perform SMB packet signing. This policy is defined by default in Local Computer Policy, where it is enabled by default.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Microsoft Network Client: Digitally sign communications (if server agrees)” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to have the SMB client sign SMB packets when possible.

Group ID (Vulid): V-1168
Group Title: Members of the Backup Operators Group
Rule ID: SV-29521r1_rule
Severity: CAT II
Rule Version (STIG-ID): 1.007
Rule Title: Members of the Backup Operators group do not have separate accounts for backup duties and normal operational tasks.

Vulnerability Discussion: Backup Operators are able to read and write to any file in the system, regardless of the rights assigned to it. Backup and restore rights permit users to cirvumvent the file access restrictions present on NTFS disk drives for the purpose of backup and restore. Members of the Backup Operators group should have special logon accounts for performing their backup duties.

Documentable: YES
Responsibility: Information Assurance Officer
IAControls: ECLP-1

Check Content:
Review the Backup Operators group in Computer Management and/or Active Directory Users and Computers. If the group contains no accounts, this is not a finding. If the group does contain any accounts, this must be documented as specified below.

Documentable Explanation: Any accounts that are members of the Backup Operators group must be documented with the IAO including application accounts. Each Backup Operator will have a separate user account for backing up the system and for performing normal user tasks.

Fix Text: Create the necessary documentation that identifies the members of this privileged group. Ensure that each member has a separate account for user duties and one for his privileged duties and the other requirements outlined in the manual check are met.

Group ID (Vulid): V-1171
Group Title: Format and Eject Removable Media
Rule ID: SV-29215r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.052
Rule Title: Ejection of removable NTFS media is not restricted to Administrators.

Vulnerability Discussion: Removable hard drives can be formatted and ejected by others who are not members of the Administrators Group, if they are not properly configured. Formatting and ejecting removable NTFS media should only be done by administrators.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Devices: Allowed to Format and Eject Removable Media” is not set to ” Administrators”, then this is a finding.

Fix Text: Configure the system to restrict ejection of removable NTFS media to "Administrators".

Group ID (Vulid): V-1172
Group Title: Password Expiration Warning
Rule ID: SV-29219r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.054
Rule Title: Users are not warned in advance that their passwords will expire.

Vulnerability Discussion: This setting configures the system to display a warning to users telling them how many days are left before their password expires. By giving the user advanced warning, the user has time to construct a sufficiently strong password.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Interactive Logon: Prompt user to change password before expiration” is not set to “14 days” or more, then this is a finding.

Fix Text: Configure the system to warn users, a minimum of 14 days in advance, that their passwords will expire.

Group ID (Vulid): V-1173
Group Title: Global System Objects Permission Strength
Rule ID: SV-29222r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.055
Rule Title: The default permissions of Global system objects are not increased.

Vulnerability Discussion: Windows system maintains a global list of shared system resources such as DOS device names, mutexes, and semaphores. Each type of object is created with a default DACL that specifies who can access the objects with what permissions. If this policy is enabled, the default DACL is stronger, allowing non-admin users to read shared objects, but not modify shared objects that they did not create.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “System Objects: Strengthen default permissions of internal system objects (e.g. Symbolic links)” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to increase permissions on internal system objects.

Group ID (Vulid): V-1174
Group Title: Idle Time Before Suspending a Session.
Rule ID: SV-29225r1_rule
Severity: CAT III
Rule Version (STIG-ID): 4.028
Rule Title: Amount of idle time required before suspending a session is improperly set.

Vulnerability Discussion: Administrators should use this setting to control when a computer disconnects an inactive SMB session. If client activity resumes, the session is automatically reestablished. This protects critical and sensitive network data from exposure to unauthorized personnel with physical access to the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Microsoft Network Server: Amount of idle time required before suspending a session” is not set to ”15 minutes” or less, then this is a finding.

Fix Text: Configure the system to suspend an idle SMB session after 15 minutes or less.

Group ID (Vulid): V-2371

Group Title: ACLs for disabled services
Rule ID: SV-29524r1_rule
Severity: CAT II
Rule Version (STIG-ID): 2.014
Rule Title: ACLs for disabled services do not conform to minimum standards.

Vulnerability Discussion: When configuring either the startup mode or access control list for a service, you must configure the other as well. When a service is explicitly disabled, its ACL should also be secured by changing the default ACL from Everyone Full Control to grant Administrators and SYSTEM Full Control and Interactive Read access.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Windows 2003/XP/Vista - Use the "Security Configuration and Analysis" snap-in to analyze the system.
Expand the “Security Configuration and Analysis” object in the tree window.
Expand the “System Services” object and select each applicable disabled Service.
(Disabled Services can be identified using the Control Panel’s Services applet.
Right click the Service and select Properties
Select ‘View Security’

If the ACLs for applicable disabled Services do not restrict permissions to Administrators, ‘full Control’, System ‘full control’, and Interactive ‘Read’, then this is a finding.

Note: These are the Windows default settings.

Fix Text: Create a Custom Security Template using the Security Template MMC Snap-in to set the permissions as required for disabled services.

Import the Custom Template into the Security Configuration and Analysis Snap-In and Select Configure Computer Now

Or import the Custom Template in to a Group Policy for application.

The administrator should have a thorough understanding of these tools before implementing settings with them.

Group ID (Vulid): V-2372
Group Title: Reversible Password Encryption
Rule ID: SV-29688r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.057
Rule Title: Reversible password encryption is not disabled.

Vulnerability Discussion: Storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords. For this reason, this policy should never be enabled.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Account Policies -> Password Policy.
If the value for “Store password using reversible encryption for all users in the domain” is not disabled, then this is a

finding.

Fix Text: Configure the system to prevent passwords from being saved using reverse encryption.

Group ID (Vulid): V-2374
Group Title: Disable Media Autoplay
Rule ID: SV-6272r4_rule
Severity: CAT I
Rule Version (STIG-ID): 3.059
Rule Title: The system is configured to autoplay removable media.

Vulnerability Discussion: Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media starts immediately. By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives. If you enable this policy, you can also disable Autoplay on all drives.

Responsibility: System Administrator
IAControls: ECLP-1, ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\

Value Name: NoDriveTypeAutorun
Type: REG_DWORD
Value: 0x000000ff (255)

Note: If the value for NoDriveTypeAutorun is entered manually, it should be entered as "ff" when Hexadecimal is selected or "255" with Decimal selected. Using the policy specified in the Fix section will enter it correctly.

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies -> "Turn off AutoPlay" to "Enabled:All Drives".

Note: This was previously configured in the checklist using the Security Option setting "MSS: (NoDriveTypeAutorun) Disable Autorun on all drives" set to "255, disable Autorun for all drives". This updates the same registry value (NoDriveTypeAutorun) as the Administrative Template.

Group ID (Vulid): V-2908
Group Title: Unencrypted Remote Access
Rule ID: SV-29695r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.061
Rule Title: Unencrypted remote access is permitted to system services.

Vulnerability Discussion: This is a category 1 finding because when unencrypted access to system services is permitted, an intruder can intercept user identification and passwords that are being transmitted in clear text. This could give an intruder unlimited access to the network.

Responsibility: Information Assurance Officer

IAControls: ECCT-1, ECCT-2

Check Content:
Interview the IAO to ensure that encryption of userid and password information is required, and data is encrypted according to DoD policy.

If the user account used for unencrypted remote access within the enclave (premise router) has administrator privileges, then this is a finding.

If userid and password information used for remote access to system services from outside the enclave is not encrypted, then this is a finding.

Fix Text: Encryption of userid and password information is required.

Encryption of the user data inside the network firewall is also highly recommended.

Encryption of user data coming from or going outside the network firewall is required.

Encryption for administrator data is always required.

Refer to the Enclave Security STIG section on "FTP and Telnet," for detailed information on its use.

Group ID (Vulid): V-3245
Group Title: File share ACLs
Rule ID: SV-29212r1_rule
Severity: CAT II
Rule Version (STIG-ID): 2.015
Rule Title: File share ACLs have not been reconfigured to remove the Everyone group.

Vulnerability Discussion: By default, the Everyone group is given full control to new file shares. When a share is created, permissions should be reconfigured to give the minimum access to those accounts that require it.

False Positives:
System created shares should be excluded from the check.

Documentable: YES
Responsibility: System Administrator
IAControls: ECAN-1

Check Content:
Run the Computer Management Applet.
Expand the "System Tools" object in the Tree window.
Expand the "Shared Folders" object.
Select the "Shares" object.
Right click any user-created shares (ignore "Netlogon", "Sysvol" and administrative shares; the system will prompt you if Properties are selected for administrative shares).
Select Properties.
Select the Share Permissions tab.

If user-created file shares have not been reconfigured to remove ACL permissions from the "Everyone group", then this is a finding.

Note: On Application Servers, if regulare users have write or delete permissions to shares containing application binary files (i.e. .exe, .dll, .cmd, etc.) this is a finding.

Documentable: If shares created by applications require the "Everyone" group, this should be documented with the IAO.

Fix Text: Remove permissions from the Everyone group from locally-created file shares and assign them to authorized groups.

Group ID (Vulid): V-3337
Group Title: Anonymous SID/Name Translation
Rule ID: SV-29701r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.062
Rule Title: Anonymous SID/Name translation is allowed.

Vulnerability Discussion: This is a Category 1 finding because this setting controls the ability of users or process that have authenticated as anonymous users to perform SID/Name translation. This setting should be disabled, as only authorized users should be able to perform such translations.

Documentable: YES
Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Network access: Allow anonymous SID/Name translation” is not set to “Disabled”, then this is a finding.

Documentable Explanation: The default setting for domain controllers is Enabled. Disabling it means that legacy systems may be unable to communicate with Windows Server 2003/2008 – based domains. This requirement should be documented with the IAO.

Fix Text: Configure the system to disable anonymous SID/Name translation.

Group ID (Vulid): V-3338
Group Title: Anonymous Access to Named Pipes
Rule ID: SV-15089r4_rule
Severity: CAT I
Rule Version (STIG-ID): 3.063
Rule Title: Unauthorized named pipes are accessible with anonymous credentials.

Vulnerability Discussion: This is a Category 1 finding because the potential for gaining unauthorized system access. Pipes are internal system communications processes. They are identified internally by ID numbers that vary between systems. To make access to these processes easier, these pipes are given names that do not vary between systems. This setting controls which of these pipes anonymous users may access.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

Windows Vista - Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for “Network access: Named pipes that can be accessed anonymously” contains entries besides “NETLOGON, Lsarpc, samr, browser”, then this is a finding.

Note: Legitimate applications may add entries to this registry value. If an application requires these entries to function properly and is documented with the IAO this would not be a finding. Documentation should contain supporting information from the vendor's instructions.

Fix Text: Configure the system to prevent unauthorized named pipes to be accessed anonymously.

Group ID (Vulid): V-3339
Group Title: Remotely AccessibleRegistry Paths
Rule ID: SV-28587r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.064
Rule Title: Unauthorized registry paths are remotely accessible.

Vulnerability Discussion: This is a Category 1 finding because it could give unauthorized individuals access to the Registry.
It controls which registry paths are accessible from a remote computer.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Windows 03/08/Vista - Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network access: Remotely accessible registry paths” contains entries besides the following, then this is a finding:

System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion

Note: Legitimate applications may add entries to this registry value. If an application requires these entries to function properly and is documented with the IAO this would not be a finding. Documentation should contain supporting information from the vendor's instructions.

Fix Text: Configure the system to restrict unauthorized remotely accessible registry paths.

Group ID (Vulid): V-3340
Group Title: Anonymous Access to Network Shares
Rule ID: SV-29703r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.065
Rule Title: Unauthorized shares can be accessed anonymously.

Vulnerability Discussion: This is a Category 1 finding because the potential for gaining unauthorized system access. Any shares listed can be accessed by any network user. This could lead to the exposure or corruption of sensitive data. Enabling this setting is very dangerous.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for "Network access: Shares that can be accessed anonymously" includes any entries, then this is a finding.

Fix Text: Configure the system to prevent shares from being accessed anonymously.

Group ID (Vulid): V-3343
Group Title: Remote Assistance - Solicit Remote Assistance
Rule ID: SV-29229r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.068
Rule Title: Solicited Remote Assistance is allowed.

Vulnerability Discussion: This setting controls whether or not solicited remote assistance is allowed from this computer. Solicited assistance is help that is specifically requested by the user. This is a Category 1 finding because it may allow unauthorized parties access to the resources on the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: fAllowToGetHelp

Type: REG_DWORD
Value: 0

Fix Text: Configure the system to disable Remote Assistance by setting the policy value for Computer Configuration -> Administrative Templates -> System -> Remote Assistance "Solicited Remote Assistance" to "Disabled".

Group ID (Vulid): V-3344
Group Title: Limit Blank Passwords
Rule ID: SV-29233r1_rule
Severity: CAT I
Rule Version (STIG-ID): 4.036
Rule Title: The use of local accounts with blank passwords is not restricted to console logons only.

Vulnerability Discussion: This is a Category 1 finding because no accounts with blank passwords should exist on

a system. The password policy should prevent this from occurring. However, if a local account with a blank password does exist, enabling this setting will limit the account to local console logon only.

Responsibility: System Administrator
IAControls: IAIA-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Accounts: Limit local account use of blank passwords to console logon only” is not set to ” Enabled”, then this is a finding.

Fix Text: Configure the system to restrict local accounts with blank passwords to console logons only.

Group ID (Vulid): V-3347
Group Title: Internet Information System (IIS)
Rule ID: SV-29706r1_rule
Severity: CAT I
Rule Version (STIG-ID): 5.016
Rule Title: Internet Information System (IIS) or its subcomponents are installed on a workstation.

Vulnerability Discussion: This is a Category 1 finding because not removing these services may allow unauthorized internet services to be hosted. Web sites should only be hosted on servers that have been designed for that purpose and can be adequately secured.

Documentable: YES
Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Select “Start”
Select “Control Panel”
Select the “Add or Remove Programs” applet.
Select “Add/Remove Windows Components”.

If the entry for “Internet Information Services” is checked, then this is a finding.

Documentable Explanation: If an application requires IIS or a subset to be installed to function, this needs be documented with the IAO. In addition, any applicable requirements from the Web Checklist must be addressed.

Fix Text: Configure the system to remove “Internet Information Services”.

Group ID (Vulid): V-3348
Group Title: Windows Messenger - Do Not Allow To Run
Rule ID: SV-29238r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.017
Rule Title: The user is allowed to launch Windows Messenger (MSN Messenger, .NET Messenger).

Vulnerability Discussion: This setting prevents the Windows Messenger client from being run.

Instant Messaging clients must be in compliance of with the Instant Messaging STIG. Windows Messenger should not be active on Windows unless the instant messaging system is a Managed Enterprise Service for unclassified data for which the DAA has approved.

Documentable: YES
Responsibility: System Administrator
IAControls: ECIM-1

Check Content:
If the following registry value doesn't exist or its value is not set to 1, then this is a finding:
Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Messenger\Client\
Value Name: PreventRun
Type: REG_DWORD
Value: 1

Documentable Explanation: If the site has a requirement for Windows Messaging and meets the conditions of the Instant Messaging STIG this needs to be documented with the IAO.

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Messenger "Do Not Allow Windows Messenger to be Run" to "Enabled".

Group ID (Vulid): V-3349
Group Title: Windows Messenger - Do Not Start Automatically
Rule ID: SV-29243r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.018
Rule Title: Windows Messenger (MSN Messenger, .NET messenger) is run at system startup.

Vulnerability Discussion: This setting prevents the automatic launch of Windows Messenger at user logon.

Instant Messaging clients must be in compliance of with the Instant Messaging STIG. Windows Messenger should not be active on Windows unless the instant messaging system is a Managed Enterprise Service for unclassified data for which the DAA has approved.

Documentable: YES
Responsibility: System Administrator
IAControls: ECIM-1

Check Content:
If the following registry value doesn't exist or its value is not set to 1, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Messenger\Client\
Value Name: PreventAutoRun
Type: REG_DWORD
Value: 1

Documentable Explanation: If the site has a requirement for Windows Messaging and meets the conditions of the Instant Messaging STIG this needs to be documented with the IAO.

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Messenger "Do Not Automatically Start Windows Messenger Initially" to "Enabled".

Group ID (Vulid): V-3373
Group Title: Maximum Machine Account Password Age
Rule ID: SV-29246r1_rule
Severity: CAT III
Rule Version (STIG-ID): 4.043
Rule Title: The maximum age for machine account passwords is not set to requirements.

Vulnerability Discussion: This setting controls the maximum password age that a machine account may have. This setting should be set to no more than 30 days, ensuring that the machine changes its password monthly.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Domain Member: Maximum Machine Account Password Age” is not set to “30”, or less, then this is a finding.

Fix Text: Configure the system to require machine account passwords to be changed a minimum of every 30 days.

Group ID (Vulid): V-3374
Group Title: Strong Session Key
Rule ID: SV-29250r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.044
Rule Title: The system is not configured to require a strong session key.

Vulnerability Discussion: This setting controls the required strength of a session key.

Potential Impacts:
Setting this value in a domain containing Windows NT or older operating systems will prevent those systems from authenticating. This setting can also prevent a system from being joined to a domain.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Domain Member: Require Strong (Windows 2000 or Later) Session Key” is not set to “Enabled”, then this is a finding.

Warning: This setting may prevent a system from being joined to a domain if not configured consistently between systems.

Fix Text: Configure the system to require the use of a strong session key.

Group ID (Vulid): V-3375
Group Title: Domain Controller authentication for unlock
Rule ID: SV-29254r1_rule
Severity: CAT III
Rule Version (STIG-ID): 4.045
Rule Title: Domain Controller authentication is not required to unlock the workstation.

Vulnerability Discussion: This setting controls the behavior of the system when you attempt to unlock the workstation. If this setting is enabled, the system will pass the credentials to the domain controller (if in a domain) for authentication before allowing the system to be unlocked. This will be set to disabled per the FDCC.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Workstations - Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for “Interactive logon: Require domain controller authentication to unlock workstation” is not set to “Disabled”, then this is a finding.

Fix Text: FDCC XP and Vista - Configure the policy as specified in the manual check.

Group ID (Vulid): V-3376
Group Title: Storage of Passwords and Credentials
Rule ID: SV-29258r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.070
Rule Title: The system is configured to permit storage of credentials or .NET Passports.

Vulnerability Discussion: This setting controls the storage of authentication credentials or .NET passports on the local system. Such credentials should never be stored on the local machine as that may lead to account compromise.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network access: Do not allow storage of credentials or .NET passports for network authentication” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to prevent the storage of credentials and .NET passports on the local system.

Group ID (Vulid): V-3377
Group Title: Everyone Permissions Apply to Anonymous
Rule ID: SV-29263r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.071

Rule Title: The system is configured to give anonymous users Everyone rights.

Vulnerability Discussion: This setting helps define the permissions that anonymous users have. If this setting is enabled then anonymous users have the same rights and permissions as the built-in Everyone group. Anonymous users should not have these permissions or rights.

Potential Impacts:
This setting will cause NT compatibility issues in mixed domains and may break cross domain trusts with Windows NT domains.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network access: Let everyone permissions apply to anonymous users” is not set to “Disabled”, then this is a finding.

Note: This setting will cause NT compatibility issues in mixed domains and may break cross domain trusts with Windows NT domains. In a mixed domain, it should be set to “Enabled”.

Fix Text: Configure the system to restrict anonymous users from the Everyone group.

Group ID (Vulid): V-3378
Group Title: Sharing and Security Model for Local Accounts
Rule ID: SV-29266r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.072
Rule Title: The system is not configured to use the Classic security model.

Vulnerability Discussion: Windows includes two network-sharing security models—Classic and Guest only. With the classic model, local accounts must be password protected; otherwise, anyone can use guest user accounts to access shared system resources.

Responsibility: System Administrator
IAControls: ECLO-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network access: Sharing and security model for local accounts” is not set to “Classic – local users authenticate as themselves”, then this is a finding.

Fix Text: Configure the system to use the Classic logon, which requires users to log on as themselves.

Group ID (Vulid): V-3379
Group Title: LAN Manager Hash Value Stored
Rule ID: SV-29269r1_rule

Severity: CAT I
Rule Version (STIG-ID): 3.073
Rule Title: The system is configured to store the LAN Manager hash of the password in the SAM.

Vulnerability Discussion: This setting controls whether or not a LAN Manager hash of the password is stored in the SAM the next time the password is changed. The LAN Manager hash is a weak encryption algorithm and there are several tools available that use this hash to retrieve account passwords.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network security: Do not store LAN Manager hash value on next password change” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to prevent the LAN Manager hash from being stored in the SAM.

Group ID (Vulid): V-3380
Group Title: Force Logoff When Logon Hours Expire
Rule ID: SV-29528r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.074
Rule Title: The system is not configured to force users to log off when their allowed logon hours expire.

Vulnerability Discussion: This setting controls whether or not users are forced to log off when their allowed logon hours expire. If logon hours are set for users, then this should be enforced.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network security: Force logoff when logon hours expire” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to log off users when their allowed logon hours expire.

Group ID (Vulid): V-3381
Group Title: LDAP Client Signing
Rule ID: SV-29272r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.075
Rule Title: The system is not configured to recommended LDAP client signing requirements.

Vulnerability Discussion: This setting controls the signing requirements for LDAP clients. This setting should be

set to Negotiate signing or Require signing depending on the environment and type of LDAP server in use.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network security: LDAP client signing requirements” is not set to at least “Negotiate signing”, then this is a finding.

Fix Text: Configure the system to, at a minimum, negotiate signing for accessing LDAP.

Group ID (Vulid): V-3382
Group Title: Session Security for NTLM SSP Based Clients
Rule ID: SV-15980r4_rule
Severity: CAT II
Rule Version (STIG-ID): 3.076
Rule Title: The system is not configured to meet the minimum requirement for session security for NTLM SSP based Clients.

Vulnerability Discussion: Starting with Windows 2000 Microsoft has implemented a variety of security support providers for use with RPC sessions. In a homogenous Windows environment, all of the options should be enabled and testing should be performed in a heterogeneous environment to determine the maximum-security level that provides reliable functionality.

Documentable: YES
Potential Impacts:
Microsoft warns that setting these may prevent the client from communicating with legacy servers that do not support them. “Require NTLMv2 session security” will prevent authentication, if the “Network security: LAN Manager authentication level” is set to permit NTLM or LM authentication.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
Vista - Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network security: Minimum session security for NTLM SSP based (including secure RPC) clients” is not set to “Require NTLMv2 session security” and ”Require 128-bit encryption” then this is a finding.

Warning: Microsoft warns that setting these may prevent the client from communicating with legacy servers that do not support them.

Warning: “Require NTLMv2 session security” will prevent authentication, if the “Network security: LAN Manager Authentication level” is set to permit NTLM or LM authentication.

Documentable Explanation: If these settings need to be modified in a mixed Windows environment, the changes should be documented with the IAO.

Fix Text: Configure the system to meet requirements for NTLM SSP based clients.

Group ID (Vulid): V-3383
Group Title: FIPS Compliant Algorithms
Rule ID: SV-29532r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.077
Rule Title: The system is not configured to use FIPS compliant Algorithms for Encryption, Hashing, and Signing.

Vulnerability Discussion: This setting ensures that the system uses algorithms that are FIPS compliant for encryption, hashing, and signing. FIPS compliant algorithms meet specific standards established by the U.S. Government and should be the algorithms used for all OS encryption functions.

Potential Impacts:
Clients with this setting enabled will not be able to communicate via digitally encrypted or signed protocols with servers that do not support these algorithms. Both the Browser and Web Server must be configured to use TLS, or the browser will not be able to connect to a secure site.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” is not set to “Enabled”, then this is a finding.

Warning: Clients with this setting enabled will not be able to communicate via digitally encrypted or signed protocols with servers that do not support these algorithms. Both the browser and web server must be configured to use TLS, or the browser will not be able to connect to a secure site.

Fix Text: Configure the system to require the use of FIPS compliant algorithms.

Group ID (Vulid): V-3385
Group Title: Case Insensitivity for Non-Windows
Rule ID: SV-29535r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.078
Rule Title: The system is configured to allow case insensitivity.

Vulnerability Discussion: This setting controls the behavior of non-Windows subsystems when dealing with the case of arguments or commands. Case sensitivity could lead to the access of files or commands that should be restricted. To prevent this from happening, case insensitivity restrictions should be required.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.

Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “System Object: Require Case Insensitivity for Non-Windows Subsystems” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to require case insensitivity for non-Windows systems.

Group ID (Vulid): V-3426
Group Title: NetMeeting Disable Remote Desktop Sharing
Rule ID: SV-29276r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.027
Rule Title: The system is configured to allow remote desktop sharing through NetMeeting.

Vulnerability Discussion: Remote desktop sharing enables several users to interact and control one desktop. This could allow unauthorized users to control the system. Remote desktop sharing should be disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or its value is not set to 1, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Conferencing\
Value Name: NoRDS
Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> NetMeeting “Disable remote Desktop Sharing” to “Enabled".

Group ID (Vulid): V-3453
Group Title: TS/RDS - Password Prompting
Rule ID: SV-29277r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.042
Rule Title: Terminal Services is not configured to always prompt a client for passwords upon connection.

Vulnerability Discussion: This setting, which is located under the Encryption and Security section of the Terminal Services configuration option, controls the ability of users to supply passwords automatically as part of their Remote Desktop Connection. Disabling this setting would allow anyone to use the stored credentials in a connection item to connect to the terminal server.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: fPromptForPassword

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services -> Encryption and Security "Always Prompt Client for Password upon Connection" to "Enabled".

Group ID (Vulid): V-3454
Group Title: TS/RDS - Set Encryption Level
Rule ID: SV-29280r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.043
Rule Title: Terminal Services is not configured with the client connection encryption set to the required level.

Vulnerability Discussion: This setting, which is located under the Encryption and Security section of the Terminal Services configuration option, controls the encryption that is used for the client connection. This setting will vary depending on the clients that are being used. If a homogenous XP environment is in use, it should be set to high. Otherwise it should be set to Client compatible.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: MinEncryptionLevel

Type: REG_DWORD
Value: 3

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services -> Encryption and Security "Set Client Connection Encryption Level" to "Enabled", and set to "high".

Group ID (Vulid): V-3455
Group Title: Terminal Services - Do Not Use Temp Folders
Rule ID: SV-16954r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.044
Rule Title: Terminal Services is configured to use a common temporary folder for all sessions.

Vulnerability Discussion: This setting, which is located under the Temporary Folders section of the Terminal Services configuration option, controls the use of per session temporary folders or of a communal temporary folder. If this setting is enabled, only one temporary folder is used for all terminal services sessions. If a communal temporary folder is used, it might be possible for users to access other users temporary folders.

Responsibility: System Administrator
IAControls: ECRC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: PerSessionTempDir

Type: REG_DWORD
Value: 1

Fix Text: 2008/Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services -> Terminal Server -> Temporary Folders "Do Not Use Temp Folders per Session" will be set to "Disabled".

Group ID (Vulid): V-3456
Group Title: Terminal Services - Delete Temp Folders
Rule ID: SV-16955r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.045
Rule Title: Terminal Services is not configured to delete temporary folders.

Vulnerability Discussion: This setting, which is located under the Temporary Folders section of the Terminal Services configuration option, controls the deletion of the temporary folders when the session is terminated. Temporary folders should always be deleted after a session is over to prevent hard disk clutter and potential leakage of information.

Responsibility: System Administrator
IAControls: ECRC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: DeleteTempDirsOnExit

Type: REG_DWORD
Value: 1

Fix Text: 2008/Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services -> Terminal Server -> Temporary Folders "Do Not Delete Temp Folder upon Exit" will be set to "Disabled".

Group ID (Vulid): V-3457
Group Title: Terminal Services - Time Limit for Disc. Session

Rule ID: SV-16613r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.046
Rule Title: Terminal Services is not configured to set a time limit for disconnected sessions.

Vulnerability Discussion: This setting, which is located under the Sessions section of the Terminal Services configuration option, controls how long a session will remain open if it is unexpectedly terminated. Such sessions should be terminated as soon as possible.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or its value is not set to 1 minute or less, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\
Value Name: MaxDisconnectionTime
Type: REG_DWORD
Value: 0x0000ea60 (60000)

Fix Text: Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services -> Terminal Server -> Session Time Limits "Set Time Limit for Disconnected Sessions" to "Enabled", and the "End a disconnected session" set to "1" minute or less.

Group ID (Vulid): V-3458
Group Title: Terminal Services - Time Limit for Idle Session
Rule ID: SV-16614r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.047
Rule Title: Terminal Services is configured to allow an Idle session limit doesnt meet the requirement.

Vulnerability Discussion: This setting, which is located under the Sessions section of the Terminal Services configuration option, controls how long a session may be idle before it is automatically disconnected from the server. Users should disconnect if they plan on being away from their terminals for extended periods of time. Idle sessions should be disconnected after 15 minutes.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or its value is not set to 15 minutes or less, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: MaxIdleTime

Type: REG_DWORD
Value: 0x000dbba0 (900000)

Fix Text: Vista/2008 - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services -> Terminal Server -> Session Time Limits "Set time limit for active but idle Terminal Services sessions" to "Enabled", and the "Idle session limit" set to 15 minutes or less.

Group ID (Vulid): V-3470
Group Title: Remote Assistance - Offer Remote Assistance
Rule ID: SV-29282r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.082
Rule Title: The system is configured to allow unsolicited remote assistance offers.

Vulnerability Discussion: This setting controls whether unsolicited offers of help to this computer are allowed. The list of users allowed to offer remote assistance to this system is accessed by pressing the Helpers button.

Documentable: YES
Mitigation Control:
Remote Assistance - Offer This is a documentable finding on workstations with the following mitigations.

- Users must be trained to include the following:
  - Who they can accept assistance offer from. Offer must be in response to help desk request or confirmed with help desk if unsolicited offer comes through.
  - Users must know how to accept request, allow view or control, and how to disconnect a remote assistance session.
  - Users needs monitor the assistance activity at the workstation while it is occurring.
- The support personnel allowed to offer assistance (helpers) must be limited and documented.
- Port 3389 should be blocked at the perimeter to prevent other access.

Accounts and groups authorized to offer remote assistance (helpers) are identified in the following registry key.

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\ RAUnsolicit\

Each Account or group will be listed under a separate value name with the value equaling the value name as in the following examples.

Value Name: Administrators
Type: REG_SZ
Value: Administrators

Value Name: TestUser
Type: REG_SZ
Value: TestUser
-->

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: fAllowUnsolicited
Type: REG_DWORD
Value: 0

Documentable: Yes

Documentable Explanation: Offer remote assistance can be enabled on workstations if mitigations are in place. This must be documented with the IAO.

Mitigations:
•Users must be trained to include the following:
oWho they can accept assistance offer from. Offer must be in response to help desk request or confirmed with help desk if unsolicited offer comes through.
oUsers must know how to accept request, allow view or control, and how to disconnect a remote assistance session.
oUsers needs monitor the assistance activity at the workstation while it is occurring.
•The support personnel allowed to offer assistance (helpers) must be limited and documented.
•Port 3389 should be blocked at the perimeter to prevent other access.

Accounts and groups authorized to offer remote assistance (helpers) are identified in the following registry key.

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\ RAUnsolicit\

Each Account or group will be listed under a separate value name with the value equaling the value name as in the following examples.

Value Name: Administrators
Type: REG_SZ
Value: Administrators

Value Name: TestUser
Type: REG_SZ
Value: TestUser

Fix Text: Configure the system to prevent unsolicited remote assistance offers by setting the policy value for Computer
Configuration -> Administrative Templates -> System -> Remote Assistance “Offer Remote Assistance” to “Disabled”.

Group ID (Vulid): V-3471
Group Title: Error Reporting - Report Errors
Rule ID: SV-29285r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.083
Rule Title: The system is configured to automatically forward error information.

Vulnerability Discussion: This setting controls the reporting of errors to Microsoft and, if defined, a corporate error reporting site. This does not interfere with the reporting of errors to the local user. Since the contents of memory are included in this Error Report, sensitive information may be transmitted to Microsoft. This feature should be disabled to prevent the release of such information.

Documentable: YES
Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\PCHealth\ErrorReporting\

Value Name: DoReport

Type: REG_DWORD
Value: 0

Documentable Explanation: This setting may be enabled, if the site has configured the options to send the report to a local error reporting server: Computer Configuration -> Administrative Templates -> System -> Error Reporting ,"Configure Error Reporting". Document the requirement with the IAO.

Fix Text: Configure the system to prevent error forwarding by setting the policy value for: Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings "Turn off Windows Error Reporting"" to "Enabled".

Group ID (Vulid): V-3472
Group Title: Windows Time Service - Configure NTP Client
Rule ID: SV-29538r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.084
Rule Title: The system is configured to use an unauthorized time server.

Vulnerability Discussion: The Windows Time Service controls time synchronization settings. Time synchronization is essential for authentication and auditing purposes. The Windows Time Service attempts to synchronize with the Microsoft time server time.windows.com. If the Windows Time Service is used, it should synchronize with a secure, authorized time source, and not the Microsoft time server.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value exists and its value is set to "time.windows.com" or other unauthorized server, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\W32time\Parameters\

Value Name: NTPServer

Type: REG_SZ
Value: any authorized url

Note: For DoD organizations, the authorized time servers are USNO NTP servers as identified at http://tycho.usno.navy.mil/ntp.html.

Note: For those versions supported by the Gold Disk, it will return a finding if "Configure Windows NTP Client" is "Enabled". Review the following registry value. If it contains an authorized time server, manually close the finding.

Fix Text: Configure the system to point to an authorized time server by setting the value for: Computer Configuration -> Administrative Templates -> System -> Windows Time Service -> Time Providers "Configure Windows NTP Client" to "Enabled", and then configure the "NtpServer" field to point to an authorized time server.

Group ID (Vulid): V-3479
Group Title: Safe DLL Search Mode
Rule ID: SV-29717r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.088
Rule Title: The system is not configured to use Safe DLL Search Mode.

Vulnerability Discussion: The default search behavior, when an application calls a function in a Dynamic Link Library (DLL), is to search the current directory followed by the directories contained in the systems path environment variable. An unauthorized DLL inserted into an applications working directory could allow malicious code to be run on the system. Creating the following registry key and setting the appropriate value forces the system to search the %Systemroot% for the DLL before searching the current directory or the rest of the path.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “MSS: Enable Safe DLL search mode (recommended)” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to use Safe DLL search mode.

Group ID (Vulid): V-3480
Group Title: Media Player - Disabe Automatic Updates
Rule ID: SV-29354r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.060
Rule Title: Media Player is configured to allow automatic checking for updates.

Vulnerability Discussion: The automatic check for updates perform by the Windows Media Player must be disabled to ensure a constant platform and to prevent the introduction of unknown/untested software on the network.

Responsibility: System Administrator
IAControls: DCSL-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsMediaPlayer\

Value Name: DisableAutoupdate

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows

Components -> Windows Media Player “Prevent Automatic Updates” to “Enabled”.

Group ID (Vulid): V-3666
Group Title: Session Security for NTLM SSP based Servers
Rule ID: SV-15981r4_rule
Severity: CAT II
Rule Version (STIG-ID): 3.089
Rule Title: The system is not configured to meet the minimum requirement for session security for NTLM SSP based Servers.

Vulnerability Discussion: Starting with Windows 2000 Microsoft has implemented a variety of security support providers for use with RPC sessions. In a homogenous Windows environment, all of the options should be enabled and testing should be performed in a heterogeneous environment to determine the maximum-security level that provides reliable functionality.

Documentable: YES
Potential Impacts:
Microsoft warns that setting these may prevent the server from communicating with legacy clients that do not support them. “Require NTLMv2 session security” will prevent authentication, if the “Network security: LAN Manager authentication level” is set to permit NTLM or LM authentication.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
2008/Vista - Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network security: Minimum session security for NTLM SSP based (including secure RPC) servers” is not set to “Require NTLMv2 session security” and ”Require 128-bit encryption”, then this is a finding.

Warning: Microsoft warns that setting these may prevent the server from communicating with legacy clients that do not support them.

Warning: “Require NTLMv2 session security” will prevent authentication, if the “Network security: LAN Manager Authentication level” is set to permit NTLM or LM authentication.

Documentable Explanation: If the required settings must be modified to support operation in a mixed Windows environment, then this should be documented with the IAO.

Fix Text: Configure the system to meet the minimum requirement for session security for NTLM SSP based servers.

Group ID (Vulid): V-3828
Group Title: Security-Related Software Patches
Rule ID: SV-29726r1_rule
Severity: CAT II
Rule Version (STIG-ID): 2.019

Rule Title: Security-related Software Patches are not applied.

Vulnerability Discussion: Major software vendors release security patches and hot fixes to their products when security vulnerabilities are discovered. It is essential that these updates be applied in a timely manner to prevent unauthorized persons from exploiting identified vulnerabilities.

The Severity code may be elevated to a Category I if patches deemed Critical have not been applied.

Security Override Guidance:
If any of the patches not installed are Microsoft 'Critical', then this should be elevated to a Category 1.

Responsibility: System Administrator
IAControls: VIVM-1

Check Content:
Verify that the site is applying all security-related patches released by Microsoft. Determine the local site method for doing this (e.g., connection to a WSUS server, local procedure, etc.).

Severity Override: If any of the patches not installed are Microsoft 'Critical', then the category code should be elevated to '1'.

Note: If a penetration scan has been run on the network, it will report findings if security-related updates are not applied. Then, this check may be marked as "Not Applicable".

Some applications (such as DMS and GCSS) use a system release process to keep systems current. If this is the case, then these systems should be at the current release.

Fix Text: Apply all Microsoft security-related patches to the Windows system.

Group ID (Vulid): V-4108
Group Title: Audit Log Warning Level
Rule ID: SV-29729r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.092
Rule Title: The system does not generate an audit event when the audit log reaches a percent full threshold.

Vulnerability Discussion: When the audit log reaches a given percent full, an audit event is written to the security log. The event ID is 523 and is recorded as a success audit under the category of System. This option may be especially useful if the audit logs are set to be cleared manually. A recommended setting would be 90 percent.

Documentable: YES
Responsibility: System Administrator
IAControls: ECRR-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for "MSS: Percentage threshold for the security event log at which the system will generate a warning" is not set to "90" or less, then this is a finding.

Documentable Explanation: If the system is configured to write to an audit server, or is configured to automatically archive full logs, this should be documented with the IAO.

Fix Text: Configure the system to generate an audit entry when the security event log reaches a 90% full (or less) threshold.

Group ID (Vulid): V-4110
Group Title: Disable IP Source Routing
Rule ID: SV-29360r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.094
Rule Title: The system is configured to allow IP source routing.

Vulnerability Discussion: Protects against IP source routing spoofing.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)” is not set to “Highest protection, source routing is completely disabled”, then this is a finding.

Fix Text: Configure the system to disable IP source routing.

Group ID (Vulid): V-4111
Group Title: Disable ICMP Redirect
Rule ID: SV-29363r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.095
Rule Title: The system is configured to redirect ICMP.

Vulnerability Discussion: When disabled, forces ICMP to be routed via shortest path first.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes” is not set to “Disabled”, then this is a finding.

Fix Text: Configure the system to disable ICMP redirection.

Group ID (Vulid): V-4112
Group Title: Disable Router Discovery
Rule ID: SV-29366r1_rule

Severity: CAT III
Rule Version (STIG-ID): 3.104
Rule Title: The system is configured to detect and configure default gateway addresses.

Vulnerability Discussion: Enables or disables the Internet Router Discovery Protocol (IRDP) used to detect and configure Default Gateway addresses on the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “MSS: (PerformRouterDiscovery) Allow IDRP to detect and configure Default Gateway addresses (could lead to DoS)” is not set to “Disabled”, then this is a finding.

Fix Text: Configure the system to prevent use of the IRDP.

Group ID (Vulid): V-4113
Group Title: TCP Connection Keep-Alive Time
Rule ID: SV-29609r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.097
Rule Title: The system is configured for a greater keep-alive time than recommended.

Vulnerability Discussion: Controls how often TCP sends a keep-alive packet in attempting to verify that an idle connection is still intact.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “MSS: How often keep-alive packets are sent in milliseconds (300,000 is recommended)” is not set to “300000 or 5 minutes (recommended)” or less, then this is a finding.

Fix Text: Configure the system to have a TCP keep-alive time of 5 minutes or less.

Group ID (Vulid): V-4116
Group Title: Name-Release Attacks
Rule ID: SV-29369r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.101
Rule Title: The system is configured to allow name-release attacks.

Vulnerability Discussion: Prevents a denial-of-service (DoS)+ attack against a WINS server. The DoS consists of sending a NetBIOS Name Release Request to the server for each entry in the servers cache, causing a response delay in the normal operation of the servers WINS resolution capability.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “MSS: (NoNameReleaseOnDemand) Allow computer to ignore NetBIOS name release requests except from WINS servers” is not set to “Enabled”, then this is a finding.

Note: The NetBIOS name for the system will no longer appear under ‘My Network Places’.

Fix Text: Configure the system to protect against name-release attacks.

Group ID (Vulid): V-4438
Group Title: TCP Data Retransmissions
Rule ID: SV-29372r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.098
Rule Title: TCP data retransmissions are not controlled.

Vulnerability Discussion: In a SYN flood attack, the attacker sends a continuous stream of SYN packets to a server, and the server leaves the half-open connections open until it is overwhelmed and no longer is able to respond to legitimate requests.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is the default)” is not set to “3” or less, then this is a finding.

Fix Text: Configure the system to control the maximum number of times that TCP retransmits unacknowledged data segments before aborting the attempt.

Group ID (Vulid): V-4442
Group Title: Screen Saver Grace Period
Rule ID: SV-29375r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.102
Rule Title: This check verifies that Windows is configured to have password protection take effect within a limited time frame when the screen saver becomes active.

Vulnerability Discussion: Allowing more than several seconds makes the computer vulnerable to a potential attack from someone walking up to the console to attempt to log onto the system before the lock takes effect.

Responsibility: System Administrator

IAControls: PESL-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)” is not set to “5” or less, then this is a finding.

Note: An issue was identified where the Security Options files and analysis templates included the registry value for this setting as a Dword type however it should have been a String value. This has been reported to Microsoft and the Security Options files and analysis templates included with the checklists have been corrected as of the December 2008 release.

Fix Text: Configure the system to enforce a screen saver grace period of 5 seconds or less.

Group ID (Vulid): V-4443
Group Title: Remotely Accessible Registry Paths and Sub-Paths
Rule ID: SV-29731r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.108
Rule Title: Unauthorized registry paths and sub-paths are remotely accessible.

Vulnerability Discussion: The registry is a database for computer configuration information, much of which is sensitive. An attacker could use this to facilitate unauthorized activities. To reduce the risk of this happening, it is also lowered by the fact that the default ACLs assigned throughout the registry are fairly restrictive and they help to protect it from access by unauthorized users.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.

Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network access: Remotely accessible registry paths and sub-paths” contains entries besides the following, then this is a finding:

Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Perflib
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
System\CurrentControlSet\Services\Eventlog
System\CurrentControlSet\Services\Sysmonlog

Note: Legitimate applications may add entries to this registry value. If an application requires these entries to function properly and is documented with the IAO, this would not be a finding. Documentation should contain

supporting information from the vendor's instructions.

Fix Text: Configure the system to prevent remote access to unauthorized registry paths and sub-paths.

Group ID (Vulid): V-4448
Group Title: Group Policy - Registry Policy Processing
Rule ID: SV-29378r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.112
Rule Title: Group Policy objects are not reprocessed if they have not changed.

Vulnerability Discussion: Enabling this setting and then selecting the Process even if the Group Policy objects have not changed option ensures that the policies will be reprocessed even if none have been changed. This way, any unauthorized changes are forced to match the domain-based group policy settings again.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> System -> Group Policy "Registry Policy Processing" will be set to "Enabled",
and the option "Process even if the Group Policy objects have not changed" selected.

If the following registry value doesn't exist or its value is not set to 0, then this is a finding:
Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Group Policy\
{35378EAC-683F-11D2-A89A-00C04FBBCFA2}\
Value Name: NoGPOListChanges
Type: REG_DWORD
Value: 0

Server 2008 may have the value under 35378EAC-683F-11D2-A89A-00C04FBBCFA2} or {B087BE9D-454F-AF9C-04291E351182}

Fix Text: Configure the system to reprocess Group Policy objects that have changed by setting the policy value for Computer Configuration -> Administrative Templates -> System -> Group Policy "Registry Policy Processing" to "Enabled",
and select the option "Process even if the Group Policy objects have not changed".

Group ID (Vulid): V-6825
Group Title: DCOM - Default Authorization Level
Rule ID: SV-29736r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.107
Rule Title: A Windows system has an incorrect default DCOM authorization level.

Vulnerability Discussion: The DCOM default authentication level has been detected to be below the required setting. If the authentication level is None, then any user can access any object on the system without authentication.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Windows XP/2003/Vista
On the command line, execute Dcomcnfg.exe.
In the Component Services window that appears navigate to Computer -> My Computer
Right-click the entry, and select the Properties button.
Select the Default Properties tab.
If the “Default Authentication Level is set to “none or Call” then this would be a finding.

Fix Text: Windows XP/2003/Vista

Fortify DCOMs default permissions so that objects continue to function under tightened security:
1. On the command line, execute Dcomcnfg.exe
2. In the Component Services window that appears navigate to Computer -> My Computer
3. Right-click the entry, and select the Properties button.
4. Select the Default Properties tab.
5. Select a Default Authentication level other than 'None' or 'Call'. Note: For sensitive systems, an authentication level of Packet Privacy is recommended.
5. Click OK.
6. Verify that DCOM objects still function properly after making changes.

Group ID (Vulid): V-6826
Group Title: DCOM - Object Registry Permission
Rule ID: SV-29543r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.108
Rule Title: A Windows system has a writable DCOM configuration.

Vulnerability Discussion: A registry key for a valid DCOM object has access permissions that allow non-administrator users to change the security settings. If DCOM security settings are inadvertently set to a low level of security, it may be possible for an attacker to execute code, possibly under the user context of the console user.In addition, an attacker could change the security on the object to allow for a future attack, such as setting the object to run as Interactive User. The Interactive User runs the application using the security context of the user currently logged on to the computer. If this option is selected and the user is not logged on, then the application will not start.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
·Using the Registry Editor, go to the following Registry key:

HKLM\Software\Classes\Appid(inherited by all subkeys)

Administrators Full
SYSTEM Full
Users Read

·If any account other than Administrators and System has greater than “read” access, then this would be a finding.

·Select each subkey and verify that it is inheriting the same permissions.
·If any subkey has permissions that are less strict than those above, then this would be a finding.

Note: Vista subkeys that have Trusted Installer with “Full” permissions are acceptable. These will typically have lesser permissions of "Read" for Administrators and System.

Fix Text: Fortify DCOMs AppId permissions so that objects continue to function under tightened security.
1. Open Registry Editor. From the Windows Start menu, select Run, type regedt32, and click OK.
2. Go to HKEY_LOCAL_MACHINE\Software\Classes\Appid.
3. Select the application that generated this vulnerability.
4. From the Security menu, select Permissions to display the Registry Key Permissions dialog box.
5. Set the permissions to Administrators - Full Control, System - Full Control, and Users - Read.
6. For maximum security, set these permissions at the AppId rootkey, and click Replace Permission on Existing Subkeys to propagate permissions to all subkeys.

Group ID (Vulid): V-6830
Group Title: DCOM - RunAs Value
Rule ID: SV-29740r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.112
Rule Title: DCOM calls are not executed under the security context of the calling user.

Vulnerability Discussion: DCOM calls are executed under the security context of the calling user by default. If the RunAs key has been altered, the DCOM calls can be executed under the user context of the currently logged in user, or as a third user. If present, the RunAs value tells the COM Service Control Manager (SCM) the name of the account under which the server is to be activated. In addition to the account name, the COM SCM must also have the password of the account. The result of a successful logon is a security context (token) for the named account that is used as the primary token for the new COM server process. Administrators should not use this method in the evaluated configuration if accountability is required, since accountability cannot be enforced.
RunAs values will be removed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
·Using the Registry Editor, go to the following Registry key:

HKLM\Software\Classes\Appid

·View each subkey in turn and verify that the RunAs value has not been added.
·If any subkey has a RunAs value, then this would be a finding.

Note: Windows components that have default Runas values such as Interactive User do not need to be changed. Windows components that have had a Runas value added or changed and non-Windows COM objects added to the system with Runas values need to be reviewed.

Fix Text: Remove any RunAs values from DCOM objects in the Registry.

Group ID (Vulid): V-6831
Group Title: Encrypting and Signing of Secure Channel Traffic
Rule ID: SV-29381r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.113
Rule Title: Outgoing secure channel traffic is not encrypted or signed.

Vulnerability Discussion: Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but not all information is encrypted. If this policy is enabled, outgoing secure channel traffic will be encrypted and signed.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to always encrypt and sign outgoing secure channel traffic.

Group ID (Vulid): V-6832
Group Title: SMB Client Packet Signing (Always)
Rule ID: SV-29384r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.114
Rule Title: The Windows Server SMB client is not enabled to always perform SMB packet signing.

Vulnerability Discussion: If this policy is enabled, it causes the Windows Server Message Block (SMB) client to perform SMB packet signing when communicating with an SMB server that is enabled or required to perform SMB packet signing.

Potential Impacts:
If the environment is a mixed one, with down-level OSs, or maintains trusts with down-level OSs, then this to the required setting could cause compatibility problems.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Microsoft Network Client: Digitally sign communications (always)” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to always sign SMB client traffic.

Group ID (Vulid): V-6833
Group Title: SMB Server Packet Signing (Always)
Rule ID: SV-29391r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.115

Rule Title: The Windows Server SMB server is not enabled to always perform SMB packet signing.

Vulnerability Discussion: If this policy is enabled, it causes the Windows Server Message Block (SMB) server to always perform SMB packet signing.

Potential Impacts:
If the environment is a mixed one, with down-level OSs, or maintains trusts with down-level OSs, then configuring this to the required setting could cause compatibility problems.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Microsoft Network Server: Digitally sign communications (always)” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system so that the SMB Server policy is set to always sign SMB packets.

Group ID (Vulid): V-6834
Group Title: Anonymous Access to Named Pipes and Shares
Rule ID: SV-29544r1_rule
Severity: CAT I
Rule Version (STIG-ID): 3.116
Rule Title: Named Pipes and Shares can be accessed anonymously.

Vulnerability Discussion: This is a Category 1 finding because of the potential for gaining unauthorized system access.

Pipes are internal system communications processes. They are identified internally by ID numbers that vary between systems. To make access to these processes easier, these pipes are given names that do not vary between systems.

When this setting is disabled, Network shares can be accessed by any network user. This could lead to the exposure or corruption of sensitive data.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for “Network access: Restrict anonymous access to Named Pipes and Shares” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system to restrict anonymous access to named pipes and shares.

Group ID (Vulid): V-6836
Group Title: Minimum Password Length

Rule ID: SV-29388r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.013
Rule Title: For systems utilizing a logon ID as the individual identifier, passwords are not at a minimum of 14-characters.

Vulnerability Discussion: Information systems not protected with strong password schemes including passwords of minimum length provide the opportunity for anyone to crack the password thus gaining access to the system and causing the device, information, or the local network to be compromised or a denial of service.

Potential Impacts:
Strong passwords may invite users to write down the passwords. Ensure that all users store passwords in a secured location.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Account Policies -> Password Policy.

If the value for the “Minimum password length,” is less than 14 characters, then this is a finding.

Fix Text: Configure all information systems to require passwords of the minimun length specified in the check.

Group ID (Vulid): V-6840
Group Title: Password Expiration
Rule ID: SV-29395r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.026
Rule Title: To the extent system capabilities permit, system mechanisms are not implemented to enforce automatic expiration of passwords and to prevent reuse.

Vulnerability Discussion: Passwords that do not expire or are reused increase the exposure of a password with greater probability of being discovered or cracked.

False Positives:
The following accounts are exempt from this check. Built-in Administrator Account Application accounts

Documentable: YES
Potential Impacts:
Enforcing passwords to be changed at regular intervals may invite users to write down the passwords each time they are required to make a change. Ensure that all users store passwords in a secured location.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Using the DUMPSEC utility:

Select “Dump Users as Table” from the “Report” menu.
Select the available fields in the following sequence, and click on the “Add” button for each entry:

UserName
SID
PswdRequired

PswdExpires
PswdLastSetTime
LastLogonTime
AcctDisabled
Groups

If any accounts listed in the user report have a “No” in the “PswdExpires” column, then this is a finding.

Note: The following command can be used on Windows 2003/2008 Active Directory if DumpSec cannot be run:

Open a Command Prompt.
Enter “Dsquery user -limit 0 | Dsget user -dn -pwdneverexpires”.
This will return a list of User Accounts with Yes/No for Pwdneverexpires.

If any accounts have "Yes", then this is a finding.
The results can be directed to a text file by adding “> filename.txt” at the end of the command

The following are exempt from this requirement:
Built-in Admiistrator Account
Application Accounts

Documentable Explanation: Accounts that meet the requirements for allowable exceptions should be documented with the IAO.

Fix Text: Configure all information systems to expire passwords.

Group ID (Vulid): V-6850
Group Title: Auditing Configuration
Rule ID: SV-16966r3_rule
Severity: CAT II
Rule Version (STIG-ID): 4.008
Rule Title: Auditing records are configured as required.

Vulnerability Discussion: Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, analyze compromises that have occurred as well as detect an attack that has begun or is about to begin. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Without an audit trail that provides information as to event that occurred and if it was successful or unsuccessful, it is difficult to analyze a series of events to determine the steps used by an attacker to compromise a system or network, or what exactly happened that led to a denial of service. Collecting data such as the successful and unsuccessful events is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Responsibility: System Administrator
IAControls: ECAR-2, ECAR-3

Check Content:
Vista -

The major audit groupings in Security Configuration and Analysis will show Not Defined in the Database Settings.

Run AuditPol.exe to view the detailed Audit Policy. Auditpol.exe is also used to set auditing subcategories. Security Option “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings” must be set to “Enabled” for the detailed auditing to be effective.

•Click Start, All Programs, Accessories, right click on Command Prompt

•Select Runas administrator
•Enter AuditPol /get /category:*

If auditing is not configured as follows this is a finding.

System
Security System Extension Success and Failure
System Integrity Success and Failure
IPSec Driver Success and Failure
Other System Events No Auditing
Security State Change Success and Failure

Logon/Logoff
Logon Success and Failure
Logoff Success
Account Lockout No Auditing
IPsec Main Mode No Auditing
IPsec Quick Mode No Auditing
IPsec Extended Mode No Auditing
Special Logon Success
Other Logon/Logoff Events No Auditing
Network Policy Server No Auditing

Object Access
File System Failure
Registry Failure
Kernel Object No Auditing
SAM No Auditing
Certification Services No Auditing
Application Generated No Auditing
Handle Manipulation No Auditing
File Share No Auditing
Filtering Platform Packet Drop No Auditing
Filtering Platform Connection No Auditing
Other Object Access Events No Auditing

Privilege Use
Sensitive Privilege Use Success and Failure
Non Sensitive Privilege Use No Auditing
Other Privilege Use Events No Auditing
Detailed Tracking
Process Termination No Auditing
DPAPI Activity No Auditing
RPC Events No Auditing
Process Creation Success

Policy Change
Audit Policy Change Success and Failure
Authentication Policy Change Success
Authorization Policy Change No Auditing
MPSSVC Rule-Level Policy Change No Auditing
Filtering Platform Policy Change No Auditing
Other Policy Change Events No Auditing

Account Management
User Account Management Success and Failure
Computer Account Management Success and Failure

Security Group Management Success and Failure
Distribution Group Management No Auditing
Application Group Management No Auditing
Other Account Management Events Success and Failure

DS Access
Directory Service Changes No Auditing
Directory Service Replication No Auditing
Detailed Directory Service Replication No Auditing
Directory Service Access No Auditing

Account Logon
Kerberos Service Ticket Operations No Auditing
Other Account Logon Events No Auditing
Kerberos Authentication Service No Auditing
Credential Validation Success and Failure

Note: To configure detailed auditing the following command is used:

Auditpol /set /subcategory:"subcategory name" /success:enable(disable) /failure:enable(disable)

Include the quotes around the subcategory name

Fix Text: Configure the system to audit categories as outlined in check procedure.

Group ID (Vulid): V-7002
Group Title: Password Requirement
Rule ID: SV-29548r1_rule
Severity: CAT I
Rule Version (STIG-ID): 4.017
Rule Title: DOD information system access does not require the use of a password.

Vulnerability Discussion: The lack of password protection enables anyone to gain access to the information system, which opens a backdoor opportunity for intruders to compromise the system as well as other resources within the same administrative domain.

Security Override Guidance:
For a DISABLED account(s) with a blank or null password, classify/downgrade this finding to a Severity Code 2 finding.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Using the DUMPSEC utility:

Select "Dump Users as Table" from the "Report" menu.
Select the available fields in the following sequence, and click on the "Add" button for each entry:
UserName
SID
PswdRequired
PswdExpires
LastLogonTime
AcctDisabled

Groups

If any accounts listed in the user report have a “No” in the “PswdRequired” column, then this is a finding.

Note: Some built-in or application-generated accounts (e.g., Guest, IWAM_, IUSR, etc.) will not have this flag set, even though there are passwords present. It can be set by entering the following on a command line: “Net user <account_name> /passwordreq:yes”.

Severity Override: For a DISABLED account(s) with a blank or null password, classify/downgrade this finding to a Category 2 finding.

Fix Text: Configure all DoD information systems to require passwords to gain access.

The password required flag can be set by entering the following on a command line: “Net user <account_name> /passwordreq:yes”.

Group ID (Vulid): V-11806
Group Title: Display of Last User Name
Rule ID: SV-29399r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.119
Rule Title: The system is configured to allow the display of the last user name on the logon screen.

Vulnerability Discussion: The user name of the last user to log onto a system will not be displayed. This eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for “Interactive logon: Do not display last user name” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the system so that the last user name is not displayed on the logon screen.

Group ID (Vulid): V-14224
Group Title: Backup Administrator Account
Rule ID: SV-29745r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.121
Rule Title: The system does not have a backup administrator account

Vulnerability Discussion: This check verifies that a backup administrator account has been created to ensure system availability in the event that no administrators are able or available to access the system. The built-in administrator account may be used for this purpose. The IAO will ensure the backup administrator account is stored in a secure location.

Responsibility: System Administrator
IAControls: ECPA-1

Check Content:
Interview the SA to determine if a backup administrator account exists and is stored with its password in a secure location.

Fix Text: Create and maintain a backup admininstrator account for emergency situations.

Group ID (Vulid): V-14225
Group Title: Administrator Account Password Changes
Rule ID: SV-29749r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.122
Rule Title: Administrator Passwords are changed when necessary.

Vulnerability Discussion: This check verifies that the passwords for the default and backup administrator accounts are changed at least annually or when any member of the administrative team leaves the organization.

Responsibility: System Administrator
IAControls: ECPA-1

Check Content:
Interview the SA or IAM to determine if the site has a policy that requires the default and backup admin passwords to be changed at least annually or when any member of the administrative team leaves the organization.

Fix Text: Define a policy for required password changes for the default and backup admin account.

Group ID (Vulid): V-14228
Group Title: Audit Access to Global System Objects
Rule ID: SV-29401r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.123
Rule Title: Audit Access to Global System Objects is not turned off.

Vulnerability Discussion: This policy setting stops the system from setting up a default system access control list for certain system objects which could create a very large number of security events filling the Security log in Windows.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for “Audit: Audit the access to global system objects” is not set to “Disabled”, then this is a finding.

Fix Text: Configure the value for “Audit: Audit the access to global system objects” to “Disabled”.

Group ID (Vulid): V-14229
Group Title: Audit Backup and Restore Privileges
Rule ID: SV-29403r1_rule
Severity: CAT II

Rule Version (STIG-ID): 3.124
Rule Title: Audit of Backup and Restore Privileges is not turned off.

Vulnerability Discussion: This policy setting stops the system from generating audit events for every file backed up or restored which could fill the Security log in Windows.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for "Audit: Audit the use of Backup and Restore privilege" is not set to "Disabled", then this is a finding.

Fix Text: Configure the value for "Audit: Audit the use of Backup and Restore privilege" to "Disabled".

Group ID (Vulid): V-14230
Group Title: Audit Policy Subcategory Setting
Rule ID: SV-14841r3_rule
Severity: CAT II
Rule Version (STIG-ID): 3.125
Rule Title: Audit policy using subcategories is enabled.

Vulnerability Discussion: This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista and 2008.

IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" is not set to "Enabled", then this is a finding.

Fix Text: Configure the setting for "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to "Enabled".

Group ID (Vulid): V-14231
Group Title: Hide Computer
Rule ID: SV-14842r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.126
Rule Title: Hide Computer from the browse list.

Vulnerability Discussion: This check verifies Windows Vista is configured to hide the computer from the browse list.

IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for "MSS: (Hidden) Hide Computer From the Browse List" is not set to "Enabled", then this is a finding.

Fix Text: Configure the setting for "MSS: (Hidden) Hide Computer From the Browse List" to "Enabled".

Group ID (Vulid): V-14232
Group Title: IPSec Exemptions
Rule ID: SV-14843r2_rule
Severity: CAT III
Rule Version (STIG-ID): 3.127
Rule Title: IPSec Exemptions are limited.

Vulnerability Discussion: This check verifies that Windows is configured to limit IPSec exemptions.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Vista\7 - Analyze the system using the Security Configuration and Analysis snap-in.

Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options.

If the value for “MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic” is not set to “Multicast, broadcast and ISAKMP exempt (best for Windows XP)”, then this is a finding.

Fix Text: Vista\7 - Configure the setting for “MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic” to “Multicast, broadcast and ISAKMP exempt (best for Windows XP)”.

Group ID (Vulid): V-14234
Group Title: UAC - Admin Approval Mode
Rule ID: SV-14845r3_rule
Severity: CAT II
Rule Version (STIG-ID): 3.129
Rule Title: User Account Control - Built In Admin Approval Mode

Vulnerability Discussion: This check verifies whether the built-in Administrator account runs in Admin Approval Mode.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for “User Account Control: Admin Approval Mode for the Built-in Administrator account” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the setting for “User Account Control: Admin Approval Mode for the Built-in Administrator account” to “Enabled”.

Group ID (Vulid): V-14235
Group Title: UAC - Admin Elevation Prompt
Rule ID: SV-17457r1_rule
Severity: CAT II
Rule Version (STIG-ID): 3.130

Rule Title: User Account Control - Behavior of elevation prompt for administrators

Vulnerability Discussion: This check verifies whether logged on administrator is prompted for consent when he attempts to complete a task that requires raised privileges.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Vista - Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for "User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode" is not set to "Prompt for consent", then this is a finding.

Fix Text: Vista - Configure the setting for "User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode" to "Prompt for consent".

Group ID (Vulid): V-14236
Group Title: UAC - User Elevation Prompt
Rule ID: SV-14847r3_rule
Severity: CAT II
Rule Version (STIG-ID): 3.131
Rule Title: User Account Control - Behavior of elevation prompt for standard users.

Vulnerability Discussion: This check verifies whether the logged on user is prompted for credentials when attempting to complete a task that requires raised privileges.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.

Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options.

If the value for "User Account Control: Behavior of the elevation prompt for standard users" is not set to "Prompt for credentials", then this is a finding.

The policy referenced configures the following registry value:

Registry Path: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: ConsentPromptBehaviorUser

Value Type: REG_DWORD
Value: 1

Fix Text: Configure the setting for "User Account Control: Behavior of the elevation prompt for standard users" to "Prompt for credentials".

Group ID (Vulid): V-14237

Group Title: UAC - Application Installations
Rule ID: SV-14848r3_rule
Severity: CAT II
Rule Version (STIG-ID): 3.132
Rule Title: User Account Control - Detect Application Installations

Vulnerability Discussion: This check verifies whether Windows responds to application installation requests by prompting for credentials.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for “User Account Control: Detect application installations and prompt for elevation” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the setting for “User Account Control: Detect application installations and prompt for elevation” to “Enabled”.

Group ID (Vulid): V-14239
Group Title: UAC - UIAccess Application Elevation
Rule ID: SV-14850r3_rule
Severity: CAT II
Rule Version (STIG-ID): 3.134
Rule Title: User Account Control - Elevate UIAccess applications that are in secure locations

Vulnerability Discussion: This check verifies whether Windows only allows applications installed in a secure location, such as the Program Files or the Windows\System32 folders, on the file system to run with elevated privileges.

IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options.

If the value for “User Account Control: Only elevate UIAccess applications that are installed in secure locations” is not set to “Enabled”, then this is a finding.

Fix Text: Configure the setting for “User Account Control: Only elevate UIAccess applications that are installed in secure locations” to “Enabled”.

Group ID (Vulid): V-14240
Group Title: UAC - All Admin Approval Mode
Rule ID: SV-14851r3_rule
Severity: CAT II
Rule Version (STIG-ID): 3.137
Rule Title: User Account Control - Run all admins in Admin Approval Mode

Vulnerability Discussion: This check verifies that UAC has not been disabled.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for "User Account Control: Run all administrators in Admin Approval Mode" is not set to "Enabled", then this is a finding.

Fix Text: Configure the setting for "User Account Control: Run all administrators in Admin Approval Mode" to "Enabled".

Group ID (Vulid): V-14241
Group Title: UAC - Secure Desktop Mode
Rule ID: SV-14852r3_rule
Severity: CAT II
Rule Version (STIG-ID): 3.135
Rule Title: User Account Control - Switch to secure desktop

Vulnerability Discussion: This check verifies that the elevation prompt is only used in secure desktop mode.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for "User Account Control: Switch to the secure desktop when prompting for elevation" is not set to "Enabled", then this is a finding.

Fix Text: Configure the setting for "User Account Control: Switch to the secure desktop when prompting for elevation" to "Enabled".

Group ID (Vulid): V-14242
Group Title: UAC - Non UAC Compliant Application Virtualization
Rule ID: SV-14853r5_rule
Severity: CAT II
Rule Version (STIG-ID): 3.136
Rule Title: User Account Control - Non UAC Compliant Application Virtualization

Vulnerability Discussion: This check verifies that non UAC compliant applications will run in virtualized file and registry entries allowing them to run.

IAControls: ECCD-1, ECCD-2

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for "User Account Control: Virtualize file and registry write failures to per-user locations" is not set to "Enabled", then this is a finding.

Fix Text: Configure the setting for "User Account Control: Virtualize file and registry write failures to per-user locations" to "Enabled".

Group ID (Vulid): V-14243
Group Title: Enumerate Administrator Accounts on Elevation

Rule ID: SV-14854r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.132
Rule Title: Require username and password to elevate a running application.

Vulnerability Discussion: This check verifies that the system is configured to always require users to type in a user name and password to elevate a running application.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\CredUI

Value Name: EnumerateAdministrators

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Credential User Interface "Enumerate administrator accounts on elevation" to "Disabled".

Group ID (Vulid): V-14247
Group Title: TS/RDS - Prevent Password Saving
Rule ID: SV-29405r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.116
Rule Title: Terminal Services / Remote Desktop Service - Prevent password saving in the Remote Desktop Client

Vulnerability Discussion: This check verifies that the system is configured to prevent Users from saving passwords in the Remote Desktop Client.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: DisablePasswordSaving

Type: REG_DWORD
Value: 1

Fix Text: Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services-> Remote Desktop Connection Client "Do not allow passwords to be saved" to "Enabled".

Group ID (Vulid): V-14248
Group Title: TS/RDS - Remote User Connections
Rule ID: SV-14859r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.117
Rule Title: Terminal Services / Remote Desktop Services - Prevent users from connecting using Terminal Servies or Remote Desktop.

Vulnerability Discussion: This check verifies that the system is configured to prevent users from connecting to a computer using Terminal Services or Remote Desktop.

Documentable: YES
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: fDenyTSConnections

Type: REG_DWORD
Value: 1

Documentable Explanation: If terminal services/remote desktop for remote administration is being used, then this would not be a finding. This requirement needs to be documented with the IAO.

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services -> Terminal Server -> Connections "Allow users to connect remotely using Terminal Services" to "Disabled.

Group ID (Vulid): V-14249
Group Title: TS/RDS - Drive Redirection
Rule ID: SV-14860r5_rule
Severity: CAT II
Rule Version (STIG-ID): 5.118
Rule Title: Terminal Services / Remote Desktop Services - Local drives prevented from sharing with Terminal Servers.

Vulnerability Discussion: This check verifies that the system is configured to prevent users from sharing the local drives on their client computers to Terminal Servers that they access.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: fDisableCdm

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services -> Terminal Server -> Device and Resource Redirection “Do not allow drive redirection” to “Enabled”.

Group ID (Vulid): V-14250
Group Title: Configure Automatic Updates
Rule ID: SV-14861r3_rule
Severity: CAT II
Rule Version (STIG-ID): 2.119
Rule Title: Prevent Automatic Updates from being run.

Vulnerability Discussion: This check verifies that the system is configured to prevent the Automatic Updates from being run.

Documentable: YES
IAControls: DCSL-1

Check Content:
If the following registry value doesn’t exist or its value is not set to 0, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\WindowsUpdate\AU\

Value Name: NoAutoUpdate
Type: REG_DWORD
Value: 1

Documentable Explanation: If the site is using a Windows Server Update Server (WSUS) to distribute software updates, and the computer is configured to point at that server, then this can be set to "Enabled". In this instance, the setting will not be considered a finding. To determine whether WSUS is being used, see if the following registry key value exists and is pointing to an organizational or DoD WSUS URL:

HKLM\Software\Policies\Microsoft\WindowsUpdate\WUServer, Reg_SZ, http://...

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update “Configure Automatic Updates” to “Disabled”.

Group ID (Vulid): V-14253
Group Title: RPC - Unathenticated RPC Clients
Rule ID: SV-29408r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.123
Rule Title: Restrict unauthenticated RPC clients.

Vulnerability Discussion: This check verifies that the system is configured to restrict unauthenticated RPC clients from connecting to the RPC server.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Rpc\

Value Name: RestrictRemoteClients

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Remote Procedure Call "Restrictions for Unauthenticated RPC clients" to "Enabled" and "Authenticated".

Group ID (Vulid): V-14254
Group Title: RPC - Endpoint Mapper Authentication
Rule ID: SV-29410r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.124
Rule Title: Client computers required to authenticate for RPC communication.

Vulnerability Discussion: This check verifies that the system is configured to force client computers to provide authentication before an RPC communication is established.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Rpc\

Value Name: EnableAuthEpResolution

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Remote Procedure Call "RPC Endpoint Mapper Client Authentication" to "Enabled.

Group ID (Vulid): V-14255
Group Title: Publish to Web
Rule ID: SV-29412r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.125
Rule Title: File and Folder Publish to Web option unavailable.

Vulnerability Discussion: This check verifies that the system is configured to make the options to publish to the

web unavailable from File and Folder Tasks in Windows folders.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Value Name: NoPublishingWizard

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication setting 'Turn off the "Publish to Web" task for files and folders' to "Enabled".

Group ID (Vulid): V-14256
Group Title: Internet Download / Online Ordering
Rule ID: SV-29415r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.126
Rule Title: Web Publishing and online ordering wizards prevented from downloading list of providers.

Vulnerability Discussion: This check verifies that the system is configured to prevent Windows from downloading a list of providers for the Web publishing and online ordering wizards.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Value Name: NoWebServices

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication setting 'Turn off Internet download for Web publishing and online ordering wizards' to "Enabled".

Group ID (Vulid): V-14257
Group Title: Windows Messenger Experience Improvement
Rule ID: SV-29417r1_rule

Severity: CAT II
Rule Version (STIG-ID): 5.127
Rule Title: Windows Messenger prevented from collecting anonymous information.

Vulnerability Discussion: This check verifies that the system is configured to prevent Windows Messenger from collecting anonymous information about how the Windows Messenger software and service is used.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Messenger\Client

Value Name: CEIP

Type: REG_DWORD
Value: 2

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication setting 'Turn off the Windows Messenger Customer Experience Improvement Program' to "Enabled".

Group ID (Vulid): V-14258
Group Title: Search Companion Content File Updates
Rule ID: SV-29419r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.128
Rule Title: Search Companion prevented from automatically downloading content updates.

Vulnerability Discussion: This check verifies that the system is configured to prevent Search Companion from automatically download content updates during local and Internet searches.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\ SearchCompanion

Value Name: DisableContentFileUpdates

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication setting 'Turn off Search Companion content file updates' to "Enabled".

Group ID (Vulid): V-14259
Group Title: Printing Over HTTP
Rule ID: SV-29421r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.129
Rule Title: Prevent printing over HTTP.

Vulnerability Discussion: This check verifies that the system is configured to prevent the client computer's ability to print over HTTP, which allows the computer to print to printers on the intranet as well as the Internet.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Printers

Value Name: DisableHTTPPrinting

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication setting 'Turn off printing over HTTP' to "Enabled".

Group ID (Vulid): V-14260
Group Title: HTTP Printer Drivers
Rule ID: SV-29423r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.130
Rule Title: Computer prevented from downloading print driver packages over HTTP.

Vulnerability Discussion: This check verifies that the system is configured to prevent the computer from downloading print driver packages over HTTP.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Printers

Value Name: DisableWebPnPDownload

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication setting 'Turn off downloading of print drivers over HTTP' to "Enabled".

Group ID (Vulid): V-14261
Group Title: Windows Update Device Drive Searching
Rule ID: SV-29425r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.131
Rule Title: Windows is prevented from using Windows Update to search for drivers.

Vulnerability Discussion: This check verifies that the system is configured to prevent Windows from searching Windows Update for device drivers when no local drivers for a device are present.

Responsibility: System Administrator
IAControls: DCSL-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\DriverSearching

Value Name: DontSearchWindowsUpdate

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication setting 'Turn off Windows Update device driver searching' to "Enabled".

Group ID (Vulid): V-14262
Group Title: IPv6 Transition
Rule ID: SV-14873r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.050
Rule Title: IPv6 will be disabled until a deliberate transition strategy has been implemented. Use of IPv6 transition technologies will be disabled.

Vulnerability Discussion: Any nodes' interface with IPv6 enabled by default presents a potential risk of traffic being transmitted or received without proper risk mitigation strategy and therefore a serious security concern.

Documentable: YES
Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Vista - Prior to transition, IPv6 will be disabled on all interfaces. If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE

Subkey: System\CurrentControlSet\Services\Tcpip6\Parameters
Value Name: DisabledComponents
Type: REG_DWORD
Value: 0xffffffff

If IPv6 transition has been implemented, the following will disable tunnel interfaces allowing native IPv6.

The Gold Disk will check for disabling all IPv6. If the transition to IPv6 has been implemented and the tunneling interfaces have been disabled, manually close the finding.

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: System\CurrentControlSet\Services\Tcpip6\Parameters
Value Name: DisabledComponents
Type: REG_DWORD
Value: 0x1

See S0-C1-imp-1 of the The Department of National Intelligence/Department of Defense (DoD) Internet Protocol version 6 (IPv6) Information Assurance Guidance for Milestone Objective 3 for additional options/information.

Documentable: If disabling IPv6 on all interfaces prior to the transition to supporting IPv6 causes issues with necessary applications or services, document this with the IAO.

Fix Text: Vista - Add the following registry key.

To disable IPv6 on all interfaces:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: System\CurrentControlSet\Services\Tcpip6\Parameters
Value Name: DisabledComponents
Type: REG_DWORD
Value: 0xffffffff

To disable all IPv6 tunneling interfaces:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: System\CurrentControlSet\Services\Tcpip6\Parameters
Value Name: DisabledComponents
Type: REG_DWORD
Value: 0x1

Group ID (Vulid): V-14267
Group Title: Power Managment - Require Password on Resume
Rule ID: SV-28513r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.133
Rule Title: Password required on resume from hibernate/suspend.

Vulnerability Discussion: This check verifies that the user is prompted for a password on resume from hibernate/suspend.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_Current_User
Subkey: \Software\Policies\Microsoft\Windows\System\Power\

Value Name: PromptPasswordOnResume

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for User Configuration -> Administrative Templates -> System ->Power Management -> "Prompt for password on resume from hibernate/suspend" to "Enabled".

Group ID (Vulid): V-14268
Group Title: Attachment Managaer - Preserve Zone Info
Rule ID: SV-29753r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.134
Rule Title: Preserve Zone information when saving attachments.

Vulnerability Discussion: This check verifies that file attachments are marked with their zone of origin allowing Windows to determine risk.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_Current_User
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Attachments\

Value Name: SaveZoneInformation

Type: REG_DWORD
Value: 2

Fix Text: Configure the policy value for User Configuration -> Administrative Templates -> Windows Components -> Attachment Manager -> "Do not preserve zone information in file attachments" to "Disabled".

Group ID (Vulid): V-14269
Group Title: Attachment Mgr - Hide Mech to Remove Zone Info
Rule ID: SV-29755r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.135
Rule Title: Hide mechanism for removing Zone information from file attachments.

Vulnerability Discussion: This check verifies that users cannot manually remove zone information from saved file attachments.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_Current_User
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Attachments\

Value Name: HideZoneInfoOnProperties

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for User Configuration -> Administrative Templates -> Windows Components -> Attachment Manager -> "Hide mechanisms to remove zone information" to "Enabled".

Group ID (Vulid): V-14270
Group Title: Attachment Mgr - Scan with Antivirus
Rule ID: SV-29757r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.136
Rule Title: Notify antivirus when file attachments are opened.

Vulnerability Discussion: This check verifies that antivirus programs are notified when a user opens a file attachment.

Responsibility: System Administrator
IAControls: ECVP-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_Current_User
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Attachments\

Value Name: ScanWithAntiVirus

Type: REG_DWORD
Value: 3

Fix Text: Configure policy value for User Configuration -> Administrative Templates -> Windows Components -> Attachment Manager -> "Notify antivirus programs when opening attachments" to "Enabled".

Group ID (Vulid): V-14271
Group Title: Application Account Passwords
Rule ID: SV-29336r1_rule
Severity: CAT II
Rule Version (STIG-ID): 4.018
Rule Title: Application account passwords length and change requirement

Vulnerability Discussion: Setting application accounts to expire may cause applications to stop functioning. The

site will have a policy that application account passwords manually generated and entered by a system administrator are changed at least annually or when a system administrator with knowledge of the password leaves the organization. Application/service account passwords will be at least 15 characters and follow complexity requirements for all passwords.

Responsibility: System Administrator
IAControls: IAIA-1

Check Content:
The site should have a local policy to ensure that passwords for application/service accounts are at least 15 characters in length and meet complexity requirements for all passwords. Application/service account passwords manually generated and entered by a system administrator must be changed at least annually or whenever a system administrator that has knowledge of the password leaves the organization.

Interview the system administrators on their policy for application/service accounts. If it does not meet the above requirements, this is a finding.

Using the DUMPSEC utility:

Select “Dump Users as Table” from the “Report” menu.
Select the available fields in the following sequence, and click on the “Add” button for each entry:

UserName
SID
PswdRequired
PswdExpires
PswdLastSetTime
LastLogonTime
AcctDisabled
Groups

If any application accounts listed in the Dumpsec user report have a date older than one year in the “PwsdLastSetTime” column, then this is a finding.

Note: The following command can be used on Windows 2003/2008 Active Directory if DumpSec cannot be run:

Open a Command Prompt.
Enter “Dsquery user -limit 0 -o rdn -stalepwd 365”.
This will return a list of User Accounts with passwords older the one year.

Fix Text: Create application/service account passwords that are at least 15 characters in length and meet complexity requirements. Change application/service account passwords that are manually generated and entered by a system administrator at least annually or whenever an administrator with knowledge of the password leaves the organization.

Group ID (Vulid): V-15505
Group Title: HBSS CMA Agent
Rule ID: SV-29559r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.140
Rule Title: The HBSS CMA Agent is not installed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Search for the file FrameworkService.exe (by default in the \Program Files\McAfee\Common Framework\ directory) and check that the version is 3 or 4.

AND verify that the Service “McAfee Framework Service” is running.

If either of these conditions do not exist, then this is a finding.

Fix Text: Deploy the CMA agent as detailed in the CTO and in accordance with the DoD IA Enterprise Solutions STIG.

Group ID (Vulid): V-15666
Group Title: Windows Peer to Peer Networking
Rule ID: SV-29427r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.202
Rule Title: Windows Peer to Peer Networking

Vulnerability Discussion: This check verifies Microsoft Peer-to-Peer Networking Service is turned off.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Peernet\

Value Name: Disabled

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Network -> Microsoft Peer-to-Peer Networking Services “Turn Off Microsoft Peer-to-Peer Networking Services” to “Enabled”.

Group ID (Vulid): V-15667
Group Title: Prohibit Network Bridge
Rule ID: SV-29429r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.203
Rule Title: Prohibit Network Bridge in Windows

Vulnerability Discussion: This check verifies the Network Bridge can not be installed and configured.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Network Connections\

Value Name: NC_AllowNetBridge_NLA

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Network -> Network Connections "Prohibit installation and configuration of Network Bridge on your DNS domain network" to "Enabled".

Group ID (Vulid): V-15669
Group Title: Prohibit Internet Connection Sharing
Rule ID: SV-29431r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.205
Rule Title: Prohibit Internet Connection Sharing

Vulnerability Discussion: This check verifies Internet Connection Sharing can not be installed and configured.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Network Connections\

Value Name: NC_ShowSharedAccessUI

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Network -> Network Connections "Prohibit use of Internet Connection Sharing on your DNS domain network" to "Enabled".

Group ID (Vulid): V-15671
Group Title: Root Certificates Update
Rule ID: SV-29433r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.213
Rule Title: Root Certificates Update

Vulnerability Discussion: This check verifies that Root Certificates will not be updated automatically from the Microsoft site.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\SystemCertificates\AuthRoot\

Value Name: DisableRootAutoUpdate

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings "Turn off Automatic Root Certificates Update" to "Enabled".

Group ID (Vulid): V-15672
Group Title: Event Viewer Events.asp Links
Rule ID: SV-29435r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.214
Rule Title: Event Viewer Events.asp Links

Vulnerability Discussion: This check verifies that Events.asp hyperlinks in Event Viewer are available.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\EventViewer\

Value Name: MicrosoftEventVwrDisableLinks

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings "Turn off Event Viewer "Events.asp" links" to "Disabled".

Group ID (Vulid): V-15673
Group Title: Internet Connection Wizard ISP Downloads
Rule ID: SV-29436r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.216
Rule Title: Internet Connection Wizard ISP Downloads

Vulnerability Discussion: This check verifies that the Internet Connection Wizard cannot download a list of Internet Service Providers (ISPs) from Microsoft.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Internet Connection Wizard\

Value Name: ExitOnMSICW

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings "Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com" to "Enabled".

Group ID (Vulid): V-15674
Group Title: Internet File Association Service
Rule ID: SV-29438r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.217
Rule Title: Disable Internet File Association Service

Vulnerability Discussion: This check verifies that unhandled file associations will not use the Microsoft Web service to find an application.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\

Value Name: NoInternetOpenWith

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings "Turn off Internet File Association service" to "Enabled".

Group ID (Vulid): V-15675
Group Title: Windows Registration Wizard

Rule ID: SV-29440r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.218
Rule Title: Windows Registration Wizard

Vulnerability Discussion: This check verifies that the Windows Registration Wizard is blocked from online registration.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Registration Wizard Control\

Value Name: NoRegistration

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings "Turn off Registration if URL connection is referring to Microsoft.com" to "Enabled".

Group ID (Vulid): V-15676
Group Title: Order Prints Online
Rule ID: SV-29613r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.219
Rule Title: Order Prints Online

Vulnerability Discussion: This check verifies that the "Order Prints Online" task is not available in Windows Explorer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\

Value Name: NoOnlinePrintsWizard

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings "Turn off the "Order Prints" picture task" to "Enabled".

Group ID (Vulid): V-15677
Group Title: Windows Movie Maker Codec Downloads
Rule ID: SV-29442r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.220
Rule Title: Windows Movie Maker Codec Downloads

Vulnerability Discussion: This check verifies that the codecs will not be automatically downloaded for Windows Movie Maker.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsMovieMaker\

Value Name: CodecDownload

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings "Turn off Windows Movie Maker automatic codec downloads" to "Enabled".

Group ID (Vulid): V-15678
Group Title: Windows Movie Maker Web Links
Rule ID: SV-29444r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.221
Rule Title: Windows Movie Maker Web Links

Vulnerability Discussion: This check verifies that the links to web sites in Windows Movie Maker will not be available.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsMovieMaker\

Value Name: Webhelp

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings “Turn off Windows Movie Maker online Web links” to “Enabled”.

Group ID (Vulid): V-15679
Group Title: Windows Movie Maker Online Hosting
Rule ID: SV-29446r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.222
Rule Title: Windows Movie Maker Online Hosting

Vulnerability Discussion: This check verifies that movies can not be sent to a video hosting provider on the web.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsMovieMaker\

Value Name: WebPublish

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings “Turn off Windows Movie Maker saving to online video hosting provider” to “Enabled”.

Group ID (Vulid): V-15680
Group Title: Classic Logon
Rule ID: SV-29448r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.223
Rule Title: Classic Logon

Vulnerability Discussion: This check verifies that users will always use the classic logon screen.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\system\

Value Name: LogonType

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Logon "Always use classic logon" to "Enabled".

Group ID (Vulid): V-15682
Group Title: RSS Attachment Downloads
Rule ID: SV-29450r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.231
Rule Title: RSS Attachment Downloads

Vulnerability Discussion: This check verifies that attachments are prevented from being downloaded from RSS feeds.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Note: For Windows XP, this check only applies if Internet Explorer 7 or later is installed.

If the following registry value doesn't exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Internet Explorer\Feeds\

Value Name: DisableEnclosureDownload

Type: REG_DWORD
Value: 1

Fix Text: Note: For Windows XP, this only applies if Internet Explorer 7 or later is installed.

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> RSS Feeds "Turn off downloading of enclosures" to "Enabled".

Group ID (Vulid): V-15683
Group Title: Windows Explorer – Shell Protocol Protected Mode
Rule ID: SV-29452r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.240
Rule Title: Windows Explorer – Shell Protocol Protected Mode

Vulnerability Discussion: This check verifies that the shell protocol is run in protected mode. (This allows applications to only open limited folders.)

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\

Value Name: PreXPSP2ShellProtocolBehavior

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Explorer "Turn off shell protocol protected mode" to "Disabled".

Group ID (Vulid): V-15684
Group Title: Windows Installer – IE Security Prompt
Rule ID: SV-29454r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.241
Rule Title: Windows Installer – IE Security Prompt

Vulnerability Discussion: This check verifies that users are notified if a web-based program attempts to install software.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Installer\

Value Name: SafeForScripting

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Installer "Disable IE security prompt for Windows Installer scripts" to "Disabled".

Group ID (Vulid): V-15685
Group Title: Windows Installer – User Control
Rule ID: SV-29456r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.242
Rule Title: Windows Installer – User Control

Vulnerability Discussion: This check verifies that users are prevented from changing installation options.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Installer\

Value Name: EnableUserControl

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Installer "Enable user control over installs" to "Disabled".

Group ID (Vulid): V-15686
Group Title: Windows Installer – Vendor Signed Updates
Rule ID: SV-29458r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.243
Rule Title: Windows Installer – Vendor Signed Updates

Vulnerability Discussion: This check verifies that users are prevented applying vendor signed updates.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Installer\

Value Name: DisableLUAPatching

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Installer "Prohibit non-administrators from applying vendor signed updates" to "Enabled".

Group ID (Vulid): V-15687
Group Title: Media Player – First Use Dialog Boxes
Rule ID: SV-29460r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.248
Rule Title: Media Player – First Use Dialog Boxes

Vulnerability Discussion: This check verifies that users are not presented with Privacy and Installation options on

first use of Windows Media Player.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsMediaPlayer\

Value Name: GroupPrivacyAcceptance

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Media Player "Do Not Show First Use Dialog Boxes" to "Enabled".

Group ID (Vulid): V-15696
Group Title: Network – Mapper I/O Driver
Rule ID: SV-16635r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.200
Rule Title: Network – Mapper I/O Driver

Vulnerability Discussion: This check verifies that the Mapper I/O network protocol driver is disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry values don't exist or are not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\LLTD\

Value Name: AllowLLTDIOOndomain
Value Name: AllowLLTDIOOnPublicNet
Value Name: EnableLLTDIO
Value Name: ProhibitLLTDIOOnPrivateNet

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Network -> Link-Layer Topology Discovery "Turn on Mapper I/O (LLTDIO) driver" to "Disabled".

Group ID (Vulid): V-15697
Group Title: Network – Responder Driver
Rule ID: SV-16636r3_rule

Severity: CAT II
Rule Version (STIG-ID): 5.201
Rule Title: Network – Responder Driver

Vulnerability Discussion: This check verifies that the Responder network protocol driver is disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry values don't exist or are not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\LLTD\

Value Name: AllowRspndrOndomain
Value Name: AllowRspndrOnPublicNet
Value Name: EnableRspndr
Value Name: ProhibitRspndrOnPrivateNet

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Network -> Link-Layer Topology Discovery "Turn on Responder (RSPNDR) driver" to "Disabled".

Group ID (Vulid): V-15698
Group Title: Network – WCN Wireless Configuration
Rule ID: SV-16637r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.206
Rule Title: Network – Windows Connect Now Wireless Configuration

Vulnerability Discussion: This check verifies that the configuration of wireless devices using Windows Connect Now is disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry values don't exist or are not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\WCN\Registrars\

Value Name: DisableFlashConfigRegistrar
Value Name: DisableInBand802DOT11Registrar
Value Name: DisableUPnPRegistrar
Value Name: DisableWPDRegistrar
Value Name: EnableRegistrars

Type: REG_Dword
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Network -> Windows Connect Now "Configuration of wireless settings using Windows Connect Now" to "Disabled".

Group ID (Vulid): V-15699
Group Title: Network – Windows Connect Now Wizards
Rule ID: SV-16638r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.207
Rule Title: Network – Windows Connect Now Wizards

Vulnerability Discussion: This check verifies that access to the Windows Connect Now wizards is disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\WCN\UI\

Value Name: DisableWcnUi

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Network -> Windows Connect Now "Prohibit Access of the Windows Connect Now wizards" to "Enabled".

Group ID (Vulid): V-15700
Group Title: Device Install – PnP Interface Remote Access
Rule ID: SV-16639r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.208
Rule Title: Device Install – PnP Interface Remote Access

Vulnerability Discussion: This check verifies that remote access to the Plug and Play interface is disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Vista/7 - If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\DeviceInstall\Settings\

Value Name: AllowRemoteRPC

Type: REG_DWORD
Value: 0

Fix Text: Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Device Installation “Allow remote access to the PnP interface” to “Disabled”.

Group ID (Vulid): V-15701
Group Title: Device Install – Drivers System Restore Point
Rule ID: SV-16640r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.209
Rule Title: Device Install – Drivers System Restore Point

Vulnerability Discussion: This check verifies that a system restore point will be created when a new device driver is installed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Vista/7 - If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\DeviceInstall\Settings\

Value Name: DisableSystemRestore

Type: REG_DWORD
Value: 0

Fix Text: Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Device Installation “Do not create a system restore point when new device driver installed” to “Disabled”.

Group ID (Vulid): V-15702
Group Title: Device Install – Generic Driver Error Report
Rule ID: SV-16641r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.210
Rule Title: Device Install – Generic Driver Error Report

Vulnerability Discussion: This check verifies that an Error Report will not be sent when a generic device driver is installed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\DeviceInstall\Settings\

Value Name: DisableSendGenericDriverNotFoundToWER

Type: REG_DWORD
Value: 1

Fix Text: Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Device Installation “Do not send a Windows Error Report when a generic driver is installed on a system” to “Enabled”.

Group ID (Vulid): V-15703
Group Title: Driver Install – Device Driver Search Prompt
Rule ID: SV-16642r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.211
Rule Title: Driver Install – Device Driver Search Prompt

Vulnerability Discussion: This check verifies that users will not be prompted to search Windows Updated for device drivers.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\DriverSearching\

Value Name: DontPromptForWindowsUpdate

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Driver Installation “Turn off Windows Update device driver search prompt” to “Enabled”.

Group ID (Vulid): V-15704
Group Title: Handwriting Recognition Error Reporting
Rule ID: SV-16643r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.215
Rule Title: Handwriting Recognition Error Reporting (Tablet PCs)

Vulnerability Discussion: This check verifies that errors in handwriting recognition on Tablet PCs are not reported to Microsoft.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE

Subkey: \Software\Policies\Microsoft\Windows\HandwritingErrorReports\

Value Name: PreventHandwritingErrorReports

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communications settings "Turn off handwriting recognition error reporting" to "Enabled".

Group ID (Vulid): V-15705
Group Title: Power Mgmt – Password Wake on Battery
Rule ID: SV-16644r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.224
Rule Title: Power Mgmt – Password Wake on Battery

Vulnerability Discussion: This check verifies that the user is prompted for a password on resume from sleep (on battery).

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51\

Value Name: DCSettingIndex

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Power Management -> Sleep Settings "Require a Password When a Computer Wakes (On Battery)" to "Enabled".

Group ID (Vulid): V-15706
Group Title: Power Mgmt – Password Wake When Plugged In
Rule ID: SV-16645r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.225
Rule Title: Power Mgmt – Password Wake When Plugged In

Vulnerability Discussion: This check verifies that the user is prompted for a password on resume from sleep (Plugged In).

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51\

Value Name: ACSettingIndex

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Power Management -> Sleep Settings "Require a Password When a Computer Wakes (Plugged In)" to "Enabled".

Group ID (Vulid): V-15707
Group Title: Remote Assistance – Session Logging
Rule ID: SV-16646r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.226
Rule Title: Remote Assistance – Session Logging

Vulnerability Discussion: This check verifies that Remote Assistance log files will be generated.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: LoggingEnabled

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Remote Assistance "Turn on session logging" to "Enabled".

Group ID (Vulid): V-15708
Group Title: Digital Locker
Rule ID: SV-16647r2_rule
Severity: CAT III
Rule Version (STIG-ID): 5.227
Rule Title: Digital Locker

Vulnerability Discussion: This check verifies that Digital Locker, a dedicated download manager can not run.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Vista - If the following registry value doesn't exist or its value is not set to "1", then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Digital Locker\

Value Name: DoNotRunDigitalLocker

Type: REG_DWORD
Value: 1

Fix Text: Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Digital Locker "Do not allow Digital Locker to run" to "Enabled".

Group ID (Vulid): V-15709
Group Title: Game Explorer Information Downloads
Rule ID: SV-16648r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.228
Rule Title: Game Explorer Information Downloads

Vulnerability Discussion: This check verifies that game information is not downloaded from Windows Metadata Services.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\GameUX\

Value Name: DownloadGameInfo

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Game Explorer "Turn off downloading of game information" to "Enabled".

Group ID (Vulid): V-15710
Group Title: Online Assistance – Untrusted Content
Rule ID: SV-16649r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.230
Rule Title: Online Assistance – Untrusted Content

Vulnerability Discussion: This check verifies that untrusted content is not rendered for online assistance.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Assistance\Client\1.0\

Value Name: NoUntrustedContent

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Online Assistance "Turn off Untrusted Content" to "Enabled".

Group ID (Vulid): V-15711
Group Title: Search – Encrypted Files Indexing
Rule ID: SV-16650r4_rule
Severity: CAT II
Rule Version (STIG-ID): 5.232
Rule Title: Search – Encrypted Files Indexing

Vulnerability Discussion: This check verifies that encrypted files are not indexed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Windows Search\

Value Name: AllowIndexingEncryptedStoresOrItems

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Search "Allow indexing of encrypted files" to "Disabled".

Group ID (Vulid): V-15712
Group Title: Search – Exchange Folder Indexing
Rule ID: SV-16651r4_rule
Severity: CAT III
Rule Version (STIG-ID): 5.233
Rule Title: Search – Exchange Folder Indexing

Vulnerability Discussion: This check verifies that mail items on a Microsoft Exchange server are not indexed

when Outlook is run in uncached mode.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Windows Search\

Value Name: PreventIndexingUncachedExchangeFolders

Type: REG_DWORD
Value: 1

Fix Text: Vista/2008 SP2 or Search 4.0 installed:
Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Search "Enable indexing uncached Exchange folders" to "Disabled".

Prior to Vista/2008 SP2 or Search 4.0 installation, the policy name is "Prevent indexing uncached Exchange folders" and will be set to "Enabled". The registry Value Name and Value referenced in the manual check remain the same.

Group ID (Vulid): V-15713
Group Title: Defender – SpyNet Reporting
Rule ID: SV-16652r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.234
Rule Title: Defender – SpyNet Reporting

Vulnerability Discussion: This check verifies that SpyNet membership is disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value exists and is set to "1" (Basic) or "2" (Advanced), this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows Defender\Spynet\

Value Name: SpyNetReporting

Type: REG_DWORD
Value: 1 or 2 = a Finding

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Defender "Configure Microsoft Spynet Reporting" to "Disabled".

Group ID (Vulid): V-15714
Group Title: Error Reporting – Logging
Rule ID: SV-16653r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.235
Rule Title: Error Reporting – Logging

Vulnerability Discussion: This check verifies that Error Reporting events will be logged in the system event log.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Windows Error Reporting\

Value Name: LoggingDisabled

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Error Reporting "Disable Logging" to "Disabled".

Group ID (Vulid): V-15715
Group Title: Error Reporting – Windows Error Reporting
Rule ID: SV-16654r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.236
Rule Title: Error Reporting – Windows Error Reporting

Vulnerability Discussion: This check verifies that Error Reporting is disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Windows Error Reporting\

Value Name: Disabled

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Error Reporting "Disable Windows Error Reporting" to "Enabled".

Group ID (Vulid): V-15716
Group Title: Error Reporting – Error Notification
Rule ID: SV-16655r1_rule
Severity: CAT III
Rule Version (STIG-ID): 5.237
Rule Title: Error Reporting – Error Notification

Vulnerability Discussion: This check verifies that users are not given a choice to report errors.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\PCHealth\ErrorReporting\DW\

Value Name: DWAllowHeadless

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Error Reporting "Display Error Notification" to "Disabled".

Group ID (Vulid): V-15717
Group Title: Error Reporting – Additional Data
Rule ID: SV-16656r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.238
Rule Title: Error Reporting – Additional Data

Vulnerability Discussion: This check verifies that additional data requests in response to Error Reporting will be declined.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Windows Error Reporting\

Value Name: DontSendAdditionalData

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Error Reporting "Do not send additional data" to "Enabled".

Group ID (Vulid): V-15718
Group Title: Windows Explorer – Heap Termination
Rule ID: SV-16657r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.239
Rule Title: Windows Explorer – Heap Termination

Vulnerability Discussion: This check verifies that heap termination on corruption is disabled. This may prevent Windows Explorer from terminating immediately from certain legacy plug-in applications.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Explorer\

Value Name: NoHeapTerminationOnCorruption

Type: REG_DWORD
Value: 0

Fix Text: Configure the The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Explorer "Turn off heap termination on corruption" to "Disabled".

Group ID (Vulid): V-15719
Group Title: Logon – Report Logon Server
Rule ID: SV-16658r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.244
Rule Title: Logon – Report Logon Server

Vulnerability Discussion: This check verifies that the user is notified whether the logon server was accessible or cached credentials were used.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: ReportControllerMissing

Type: REG_DWORD
Value: 1

Fix Text: Configure the The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Logon Options "Report when logon server was not available during user logon" to "Enabled".

Group ID (Vulid): V-15720
Group Title: Windows Mail – Communities
Rule ID: SV-16659r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.245
Rule Title: Windows Mail – Communities

Vulnerability Discussion: This check verifies that Windows Mail will not check newsgroups for Communities support.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows Mail\

Value Name: DisableCommunities

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Mail "Turn off the communities features" to "Enabled"

Group ID (Vulid): V-15721
Group Title: Windows Mail – Disable Application
Rule ID: SV-16660r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.246
Rule Title: Windows Mail – Disable Application

Vulnerability Discussion: This check verifies that Windows Mail will be disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows Mail\

Value Name: ManualLaunchAllowed

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Mail “Turn off Windows Mail application” to “Enabled”

Group ID (Vulid): V-15722
Group Title: Media DRM – Internet Access
Rule ID: SV-16661r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.247
Rule Title: Media DRM – Internet Access

Vulnerability Discussion: This check verifies that Windows Media Digital Rights Management will be prevented from accessing the internet.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WMDRM\

Value Name: DisableOnline

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Media Digital Rights Management “Prevent Windows Media DRM Internet Access” to “Enabled”.

Group ID (Vulid): V-15723
Group Title: Meeting Space
Rule ID: SV-16662r1_rule
Severity: CAT II
Rule Version (STIG-ID): 5.249
Rule Title: Meeting Space

Vulnerability Discussion: This check verifies that Windows Meeting Space is disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Vista - If the following registry value doesn’t exist or its value is not set to “1”, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\Windows Collaboration\

Value Name: TurnOffWindowsCollaboration

Type: REG_DWORD
Value: 1

Fix Text: Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Meeting Space "Turn off Windows Meeting Space" to "Enabled"

Group ID (Vulid): V-15724
Group Title: Gadgets – Unsigned Gadgets
Rule ID: SV-16663r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.250
Rule Title: Gadgets – Unsigned Gadgets

Vulnerability Discussion: This check verifies that unsigned Gadgets will not be installed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or its value is not set to "about:blank", then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar\

Value Name: TurnOffUnsignedGadgets

Type: REG_DWORD
Value: 1

Fix Text: Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Sidebar "Disable unpacking and installation of gadgets that are not digitally signed" to "Enabled"

Group ID (Vulid): V-15725
Group Title: Gadgets – More Gadgets Link
Rule ID: SV-16664r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.251
Rule Title: Gadgets – More Gadgets Link

Vulnerability Discussion: This check verifies that the More Gadgets Link will effectively be disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified. this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar\

Value Name: OverrideMoreGadgetsLink

Type: REG_SZ
Value: Enabled:Blank

Fix Text: Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Sidebar "Override the More Gadgets Link" to "Enabled with "about:blank" entered in the option.

Group ID (Vulid): V-15726
Group Title: Gadgets – User Installed Gadgets
Rule ID: SV-16665r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.252
Rule Title: Gadgets – User Installed Gadgets

Vulnerability Discussion: This check verifies that Windows Sidebar will not run any user installed gadgets.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar\

Value Name: TurnOffUserInstalledGadgets

Type: REG_DWORD
Value: 1

Fix Text: Vista - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Sidebar "Turn Off User Installed Windows Sidebar Gadgets" to "Enabled"

Group ID (Vulid): V-15727
Group Title: User Network Sharing
Rule ID: SV-16666r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.253
Rule Title: User Network Sharing

Vulnerability Discussion: This check verifies that users are prevented from sharing files.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

Note: This setting is in HKEY_CURRENT_USER, not HKEY_LOCAL_MACHINE

If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_CURRENT_USER
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\

Value Name: NoInPlaceSharing

Type: REG_DWORD
Value: 1

Fix Text: Note: This setting is under USER Configuration not COMPUTER Configuration

Configure the policy value for User Configuration -> Administrative Templates -> Windows Components -> Network Sharing "Prevent users from sharing files within their profile" to "Enabled".

Group ID (Vulid): V-15823
Group Title: Software Certificate Installation Files
Rule ID: SV-29464r1_rule
Severity: CAT II
Rule Version (STIG-ID): 2.021
Rule Title: Remove Software Certificate Installation Files

Vulnerability Discussion: This check verifies that software certificate installation files have been removed from a system.

Documentable: YES
Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Search all drives for *.p12 and *.pfx files.

If any files with these extensions exist, then this is a finding.

Documentable Explanation: This does not apply to server-based applications that have a requirement for .p12 certificate files (e.g., Oracle Wallet Manager). Some applications create files with extensions of .p12 that are NOT certificate installation files. Removal from systems of non-certificate installation files are not required. These should be documented with the IAO.

Fix Text: Remove any certificate installation files found on a system.

Note: This does not apply to server-based applications that have a requirement for .p12 certificate files (e.g., Oracle Wallet Manager)

Group ID (Vulid): V-16007
Group Title: 8dot3 Name Creation
Rule ID: SV-29615r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.139

Rule Title: 8dot3 Name Creation Prevented

Vulnerability Discussion: This check verifies Windows is configured to allow the generation of 8.3 style file names per the FDCC.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.

Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options.

If the value for “MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)” is not set to “Disabled”, then this is a finding.

Fix Text: Configure the policy as specified in the manual check to allow the creation of 8.3 style names.

Group ID (Vulid): V-16020
Group Title: Windows Customer Experience Improvement Program
Rule ID: SV-16976r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.254
Rule Title: Windows Customer Experience Improvement Program is disabled.

Vulnerability Discussion: This check verifies that the Windows Customer Experience Improvement Program is disabled so information is not passed to the vendor.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_Local_Machine
Subkey: \Software\Policies\Microsoft\SQMClient\Windows

Value Name: CEIPEnable

Type: REG_DWORD
Value: 0

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication Settings -> “Turn off Windows Customer Experience Improvement Program” to “Enabled”.

Group ID (Vulid): V-16021
Group Title: Help Experience Improvement Program
Rule ID: SV-16977r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.255

Rule Title: Help Experience Improvement Program is disabled.

Vulnerability Discussion: This check verifies that the Windows Help Experience Improvement Program is disabled to prevent information from being passed to the vendor.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_Current_User
Subkey: \Software\Policies\Microsoft\Assistance\Client\1.0

Value Name: NoImplicitFeedback

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for User Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication Settings -> "Turn off Help Experience Improvement Program" to "Enabled".

Group ID (Vulid): V-16047
Group Title: Built-in Admin Account Status
Rule ID: SV-17029r2_rule
Severity: CAT II
Rule Version (STIG-ID): 4.039
Rule Title: Built-in Admin Account Status

Vulnerability Discussion: This check verifies that Windows Vista is configured to disable the built-in administrator account which provides no accountability.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.

If the value for "Accounts: Administrator account status" is not set to "Disabled", then this is a finding.

Fix Text: Configure the system to disable the built-in administrator account.

Group ID (Vulid): V-16048
Group Title: Help Ratings
Rule ID: SV-17030r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.256
Rule Title: Disable Help Ratings feed back.

Vulnerability Discussion: This check verifies that the users cannot provide ratings feedback to Microsoft for Help

content

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_Current_User
Subkey: \Software\Policies\Microsoft\Assistance\Client\1.0

Value Name: NoExplicitFeedback

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for User Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication Settings -> "Turn off Help Ratings" to "Enabled".

Group ID (Vulid): V-17373
Group Title: Secure Removable Media – CD-ROM
Rule ID: SV-29466r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.004
Rule Title: Secure Removable Media – CD-ROM

Vulnerability Discussion: This check verifies that Windows is configured to not limit access to CD drives when a user is logged on locally per the FDCC.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in.
Expand the Security Configuration and Analysis tree view.
Navigate to Local Policies -> Security Options.
If the value for "Devices: Restrict CD-ROM access to locally logged-on user only" is not set to "Disabled", then this is a finding.

Fix Text: Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. Set the value for "Devices: Restrict floppy access to locally logged-on user only" to "Disabled".

Group ID (Vulid): V-17374
Group Title: UAC – Executable Elevation
Rule ID: SV-18428r1_rule
Severity: CAT III
Rule Version (STIG-ID): 3.141
Rule Title: User Account Control – Executable Elevation

Vulnerability Discussion: This check verifies that elevation of application in UAC is not restricted to signed and validated applications per the FDCC.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view. Navigate to Local Policies -> Security Options. If the value for "User Account Control: Only elevate executables that are signed and validated" is not set to "Disabled", then this is a finding.

Fix Text: Configure the setting for "User Account Control: Only elevate executables that are signed and validated" to "Disabled".

Group ID (Vulid): V-17415
Group Title: Windows Firewall Domain - Enable Firewall
Rule ID: SV-18471r3_rule
Severity: CAT II
Rule Version (STIG-ID): 5.450
Rule Title: Windows Firewall Domain Profile - Enable Firewall

Vulnerability Discussion: This check enables the firewall when connected to the domain.

The domain profile settings are used when the system is connected to a network that contains domain controllers for the domain of which the computer is a member.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\

Value Name: EnableFirewall

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> State, "Firewall State" to "On (recommended)".

Group ID (Vulid): V-17416
Group Title: Windows Firewall Private - Enable Firewall

Rule ID: SV-18472r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.451
Rule Title: Windows Firewall Private Profile - Enable Firewall

Vulnerability Discussion: This check enables the firewall when connected to a private network.

The private profile is one of two options when a system is not connected to the Domain. The type is selected by the user when a new network is detected – Private for a trusted non-domain network, Public for a non-trusted non-domain network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\

Value Name: EnableFirewall

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> State, "Firewall State" to "On (recommended)".

Group ID (Vulid): V-17417
Group Title: Windows Firewall Public - Enable Firewall
Rule ID: SV-18473r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.452
Rule Title: Windows Firewall Public Profile - Enable Firewall

Vulnerability Discussion: This check enables the firewall when connected to a public network.

The public profile is one of two options when a system is not connected to the Domain. The type is selected by the user when a new network is detected – Private for a trusted non-domain network, Public for a non-trusted non-domain network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE

Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\

Value Name: EnableFirewall

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> State, “Firewall State” to “On (recommended)”.

Group ID (Vulid): V-17418
Group Title: Windows Firewall Domain - Inbound
Rule ID: SV-18474r2_rule
Severity: CAT I
Rule Version (STIG-ID): 5.453
Rule Title: Windows Firewall Domain Profile - Inbound Connections

Vulnerability Discussion: Unsolicited inbound connections for which there is no rule allowing the connection will be blocked in the domain.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\

Value Name: DefaultInboundAction

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> State, “Inbound Connections” to “Block (default)”.

Group ID (Vulid): V-17419
Group Title: Windows Firewall Domain - Outbound
Rule ID: SV-18475r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.454
Rule Title: Windows Firewall Domain Profile - Outbound Connections

Vulnerability Discussion: Outbound connections are allowed in the domain unless a rule explicitly blocks the connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\

Value Name: DefaultOutboundAction

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> State, "Outbound Connections" to "Allow (default)".

Group ID (Vulid): V-17420
Group Title: Windows Firewall Domain - Display Notifications
Rule ID: SV-18476r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.455
Rule Title: Windows Firewall Domain Profile - Display Notifications

Vulnerability Discussion: The display of notifications to the user is enabled when a program is blocked from receiving an inbound connection in the domain.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\

Value Name: DisableNotifications

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> Settings (select Customize) -> Firewall settings, “Display Notifications” to “Yes (default)”.

Group ID (Vulid): V-17421
Group Title: Windows Firewall Domain - Unicast Response
Rule ID: SV-18477r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.456
Rule Title: Windows Firewall Domain Profile - Unicast Response

Vulnerability Discussion: This check blocks unicast responses to multicast or broadcast messages in the domain.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\

Value Name: DisableUnicastResponsesToMulticastBroadcast

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> Settings (select Customize) -> Unicast response, “Allow unicast response” to “No”.

Group ID (Vulid): V-17422
Group Title: Windows Firewall Domain - Local Firewall Rules
Rule ID: SV-18478r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.457
Rule Title: Windows Firewall Domain Profile - Apply Local Firewall Rules

Vulnerability Discussion: This check ensures local firewall rules will not be merged with Group Policy settings in the domain.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\

Value Name: AllowLocalPolicyMerge

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> Settings (select Customize) -> Rule merging, "Apply local firewall rules" to "No".

Group ID (Vulid): V-17423
Group Title: Windows Firewall Domain - Local Connection Rules
Rule ID: SV-18479r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.458
Rule Title: Windows Firewall Domain Profile - Apply Local Connection Rules

Vulnerability Discussion: This check ensures local connection rules will not be merged with Group Policy settings in the domain.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\

Value Name: AllowLocalIPsecPolicyMerge

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> Settings (select Customize) -> Rule merging, “Apply local connection security rules” to “No”.

Group ID (Vulid): V-17424
Group Title: Windows Firewall Domain - Log File
Rule ID: SV-18480r2_rule
Severity: CAT III
Rule Version (STIG-ID): 5.459
Rule Title: Windows Firewall Domain Profile - Log File

Vulnerability Discussion: This check sets the location and file name of the firewall log for a domain connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging\

Value Name: LogFilePath

Type: REG_SZ
Value: %windir%\system32\logfiles\firewall\domainfirewall.log

Note: The Gold Disk will search for the file name specified in the check. If the site uses a different name for the log file, the finding will need to be closed manually.

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> Logging (select Customize), “Name” to “%

windir%\system32\logfiles\firewall\domainfirewall.log".

Group ID (Vulid): V-17425
Group Title: Windows Firewall Domain - Log Size
Rule ID: SV-18481r2_rule
Severity: CAT III
Rule Version (STIG-ID): 5.460
Rule Title: Windows Firewall Domain Profile - Log Size

Vulnerability Discussion: This check sets the firewall log file size for a domain connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging\

Value Name: LogFileSize

Type: REG_DWORD
Value: 16384 (or greater)

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> Logging (select Customize), "Size limit (KB):" to "16,384" (or greater).

Group ID (Vulid): V-17426
Group Title: Windows Firewall Domain - Log Dropped Packets
Rule ID: SV-18482r2_rule
Severity: CAT III
Rule Version (STIG-ID): 5.461
Rule Title: Windows Firewall Domain Profile - Log Dropped Packets

Vulnerability Discussion: This check enables logging of dropped packets for a domain connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE

Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging\

Value Name: LogDroppedPackets

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> Logging (select Customize), “Log dropped packets” to “Yes”.

Group ID (Vulid): V-17427
Group Title: Windows FW Domain - Log Successful Connections
Rule ID: SV-18483r2_rule
Severity: CAT III
Rule Version (STIG-ID): 5.462
Rule Title: Windows Firewall Domain Profile - Log Sucessful Connections

Vulnerability Discussion: This check enables logging of successful connections for a domain connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging\

Value Name: LogSuccessfulConnections

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Note: If the system in not a member of a domain, the Domain Profile requirements can be marked Not Applicable.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Domain Profile Tab -> Logging (select Customize), “Log successful connections” to “Yes”.

Group ID (Vulid): V-17428
Group Title: Windows Firewall Private – Inbound
Rule ID: SV-18484r2_rule
Severity: CAT I
Rule Version (STIG-ID): 5.463
Rule Title: Windows Firewall Private Profile – Inbound

Vulnerability Discussion: Unsolicited inbound connections for which there is no rule allowing the connection will be blocked on a private network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\

Value Name: DefaultInboundAction

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> State, "Inbound connections" to "Block (default)".

Group ID (Vulid): V-17429
Group Title: Windows Firewall Private - Outbound
Rule ID: SV-18485r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.464
Rule Title: Windows Firewall Private Profile - Outbound

Vulnerability Discussion: Outbound connections are allowed on a private network unless a rule explicitly blocks the connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\

Value Name: DefaultOutboundAction

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> State, “Outbound connections” to “Allow (default)”.

Group ID (Vulid): V-17430
Group Title: Windows Firewall Private - Display Notifications
Rule ID: SV-18486r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.465
Rule Title: Windows Firewall Private Profile - Display Notifications

Vulnerability Discussion: The display of notifications to the user is enabled when a program is blocked from receiving an inbound connection on a private network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\

Value Name: DisableNotifications

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> Settings (select Customize) -> Firewall settings, “Display a notification” to “Yes (default)”.

Group ID (Vulid): V-17431
Group Title: Windows Firewall Private - Unicast Response
Rule ID: SV-18487r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.466
Rule Title: Windows Firewall Private Profile - Unicast Response

Vulnerability Discussion: This check blocks unicast responses to multicast or broadcast messages on a private

network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\

Value Name: DisableUnicastResponsesToMulticastBroadcast

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> Settings (select Customize) -> Unicast response, "Allow unicast response" to "No".

Group ID (Vulid): V-17432
Group Title: Windows Firewall Private - Local Firewall Rules
Rule ID: SV-18488r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.467
Rule Title: Windows Firewall Private - Apply Local Firewall Rules

Vulnerability Discussion: This check ensures that local firewall rules will not be merged with Group Policy settings on a private network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\

Value Name: AllowLocalPolicyMerge

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> Settings (select Customize) -> Rule merging,

“Apply local firewall rules” to “No”.

Group ID (Vulid): V-17433
Group Title: Windows Firewall Private - Local Connection Rules
Rule ID: SV-18489r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.468
Rule Title: Windows Firewall Private Profile - Apply Local Connection Rules

Vulnerability Discussion: This check ensures that local connection rules will not be merged with Group Policy settings on a private network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\

Value Name: AllowLocalIPsecPolicyMerge

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> Settings (select Customize) -> Rule merging, “Apply local connection security rules” to “No”.

Group ID (Vulid): V-17434
Group Title: Windows Firewall Private - Log File
Rule ID: SV-18490r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.469
Rule Title: Windows Firewall Private Profile - Log File

Vulnerability Discussion: This check sets location and file name of the firewall log for a private network connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging

Value Name: LogFilePath

Type: REG_SZ
Value: %windir%\system32\logfiles\firewall\privatefirewall.log

Note: The Gold Disk will search for the file name specified in the check. If the site uses a different name for the log file, the finding will need to be closed manually.

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> Logging (select Customize), "Name" to "% windir%\system32\logfiles\firewall\privatefirewall.log".

Group ID (Vulid): V-17435
Group Title: Windows Firewall Private - Log Size
Rule ID: SV-18491r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.470
Rule Title: Windows Firewall Private Profile - Log Size

Vulnerability Discussion: This check sets the firewall log file size for a private network connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging

Value Name: LogFileSize

Type: REG_DWORD
Value: 16384 (or greater)

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> Logging (select Customize), "Size limit (KB)" to "16,384" (or greater).

Group ID (Vulid): V-17436

Group Title: Windows Firewall Private - Log Dropped Packets
Rule ID: SV-18492r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.471
Rule Title: Windows Firewall Private Profile - Log Dropped Packets

Vulnerability Discussion: This check enables logging of dropped packets for a private network connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging

Value Name: LogDroppedPackets

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> Logging (select Customize), "Log dropped packets" to "Yes".

Group ID (Vulid): V-17437
Group Title: Windows FW Private - Log Successful Connections
Rule ID: SV-18493r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.472
Rule Title: Windows Firewall Private Profile - Log Successful Connections

Vulnerability Discussion: This check enables logging of successful connections for a private network connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging

Value Name: LogSuccessfulConnections

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used

remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Private Profile Tab -> Logging (select Customize), "Logged successful connections" to "Yes".

Group ID (Vulid): V-17438
Group Title: Windows Firewall Public – Inbound
Rule ID: SV-18494r2_rule
Severity: CAT I
Rule Version (STIG-ID): 5.473
Rule Title: Windows Firewall Public Profile – Inbound

Vulnerability Discussion: Unsolicited inbound connections for which there is no rule allowing the connection will be blocked on a public network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\

Value Name: DefaultInboundAction

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> State, "Inbound connections" to "Block (default)".

Group ID (Vulid): V-17439
Group Title: Windows Firewall Public - Outbound
Rule ID: SV-18495r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.474
Rule Title: Windows Firewall Public Profile - Outbound

Vulnerability Discussion: Outbound connections are allowed on a public network unless a rule explicitly blocks the connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\

Value Name: DefaultOutboundAction

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> State, "Outbound connections" to "Allow (default)".

Group ID (Vulid): V-17440
Group Title: Windows Firewall Public - Display Notifications
Rule ID: SV-18496r3_rule
Severity: CAT III
Rule Version (STIG-ID): 5.475
Rule Title: Windows Firewall Public Profile - Display Notifications

Vulnerability Discussion: The display of notifications to the user is enabled when a program is blocked from receiving an inbound connection on a public network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\

Value Name: DisableNotifications

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> Settings (select Customize) -> Firewall settings, "Display a notification" to "Yes (default)".

Group ID (Vulid): V-17441
Group Title: Windows Firewall Public - Unicast Response
Rule ID: SV-18497r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.476
Rule Title: Windows Firewall Public Profile - Unicast Response

Vulnerability Discussion: This check blocks unicast responses to multicast or broadcast messages on a public network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\

Value Name: DisableUnicastResponsesToMulticastBroadcast

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> Settings (select Customize) -> Unicast response, "Allow unicast response" to "No".

Group ID (Vulid): V-17442
Group Title: Windows Firewall Public - Local Firewall Rules
Rule ID: SV-18498r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.477
Rule Title: Windows Firewall Public Profile - Apply Local Firewall Rules

Vulnerability Discussion: This check ensures that local firewall rules will not be merged with Group Policy settings on a public network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\

Value Name: AllowLocalPolicyMerge

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> Settings (select Customize) -> Rule merging, "Apply local firewall rules" to "No".

Group ID (Vulid): V-17443
Group Title: Windows Firewall Public - Local Connection Rules
Rule ID: SV-18499r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.478
Rule Title: Windows Firewall Public Profile - Apply Local Connection Rules

Vulnerability Discussion: This check ensures that local connection rules will not be merged with Group Policy settings on a public network.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\

Value Name: AllowLocalIPsecPolicyMerge

Type: REG_DWORD
Value: 0

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> Settings (select Customize) -> Rule merging, "Apply local connection security rules" to "No".

Group ID (Vulid): V-17444
Group Title: Windows Firewall Public - Log File
Rule ID: SV-18500r2_rule
Severity: CAT III
Rule Version (STIG-ID): 5.479
Rule Title: Windows Firewall Public Profile - Log File

Vulnerability Discussion: This check sets the location and file name of the firewall log for a public network

connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\

Value Name: LogFilePath

Type: REG_SZ
Value: %windir%\system32\logfiles\firewall\publicfirewall.log

Note: The Gold Disk will search for the file name specified in the check. If the site uses a different name for the log file, the finding will need to be closed manually.

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> Logging (select Customize), "Name" to "% windir%\system32\logfiles\firewall\publicfirewall.log".

Group ID (Vulid): V-17445
Group Title: Windows Firewall Public - Log Size
Rule ID: SV-18501r2_rule
Severity: CAT III
Rule Version (STIG-ID): 5.480
Rule Title: Windows Firewall Public Profile - Log Size

Vulnerability Discussion: This check sets the firewall log file size for a public network connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\

Value Name: LogFileSize

Type: REG_DWORD
Value: 16,384 (or greater)

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings ->

Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> Logging (select Customize), “Size limit (KB)” to “16,384” (or greater).

Group ID (Vulid): V-17446
Group Title: Windows Firewall Public - Log Dropped Packets
Rule ID: SV-18502r2_rule
Severity: CAT III
Rule Version (STIG-ID): 5.481
Rule Title: Windows Firewall Public Profile - Log Dropped Packets

Vulnerability Discussion: This check enables logging of dropped packets for a public network connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\

Value Name: LogDroppedPackets

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> Logging (select Customize), “Log dropped packets” to “Yes”.

Group ID (Vulid): V-17447
Group Title: Windows FW Public - Log Successful Connections
Rule ID: SV-18503r2_rule
Severity: CAT III
Rule Version (STIG-ID): 5.482
Rule Title: Windows Firewall Public Profile - Log Successful Connections

Vulnerability Discussion: This check enables logging of successful connections for a public network connection.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\

Value Name: LogSuccessfulConnections

Type: REG_DWORD
Value: 1

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Windows Firewall Properties (this link will be in the right pane) -> Public Profile Tab -> Logging (select Customize), "Logged successful connections" to "Yes".

Group ID (Vulid): V-17448
Group Title: Windows Firewall - IPv6 Block Protocols 41
Rule ID: SV-18504r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.483
Rule Title: Windows Firewall Outbound Rule - IPv6 Block Protocols 41

Vulnerability Discussion: IPv6 Transition technologies will be blocked (IPv6 Block of Protocols 41)

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Outbound Rules "IPv6 Block of Protocols 41" will be configured as follows. (The rule could have been created with a different name – view the properties to determine correct settings.)

Navigate to the rule, right click and select Properties. View the following on the tabs specified:

General: Enabled and Block the connections
Programs and Services: All programs that meet the specified conditions
Protocols and Ports: Protocol type - IPv6
Scope: Any IP addresses (Local and Remote)
Advanced: All profiles

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Add the rule with the following steps:
Navigate to Outbound Rules.
Right click in right pane and select "New Rule".
Select "Custom", Next.
Select "All Programs", Next.
Select Protocol Type: IPv6 (Protocol number 41 will be automatically selected).
Select "Any IP address" for both local and remote IP address this rule will match.
Next.
Select "Block the connection", Next.
Select all (Domain, Private and Public) for When does this rule apply?

Next.
Supply the Name: IPv6 Block of Protocols 41.
Finish.

Group ID (Vulid): V-17449
Group Title: Windows Firewall - IPv6 Block UDP 3544
Rule ID: SV-18505r2_rule
Severity: CAT II
Rule Version (STIG-ID): 5.484
Rule Title: Windows Firewall Outbound Rules - IPv6 Block UDP 3544

Vulnerability Discussion: IPv6 Transition technologies will be blocked (IPv6 Block of UDP 3544)

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Outbound Rules "IPv6 Block of UDP 3544" will be configured as follows. (The rule could have been created with a different name – view the properties to determine correct settings.)

Navigate to the rule, right click and select Properties. View the following on the tabs specified:

General: Enabled and Block the connections
Programs and Services: All programs that meet the specified conditions
Protocols and Ports: Protocols type - UDP, Local port - 3544, Remote port - All Ports
Scope: Any IP addresses (Local and Remote)
Advanced: All profiles

Note: If a third-party firewall is used, document this with the IAO and mark the Windows firewall settings as Not Applicable. The Desktop/Secure Remote Computing STIGs contain additional requirements for systems used remotely.

Fix Text: Add the rule with the following steps:
Navigate to Outbound Rules.
Right click in right pane and select "New Rule".
Select "Port", Next.
Select "All Programs", Next.
Select Protocol Type: UDP.
Select Local Port: Specific Ports, Enter 3544.
Select Remote Port: All Ports, Next.
Select "Any IP address" for both local and remote IP address this rule will match.
Next.
Select "Block the connection", Next.
Select all (Domain, Private and Public) for When does this rule apply?
Next.
Supply the Name: IPv6 Block of UDP 3544.
Finish.

Group ID (Vulid): V-17900

Group Title: Disallow AutoPlay/Autorun from Autorun.inf
Rule ID: SV-29584r1_rule
Severity: CAT I
Rule Version (STIG-ID): 2.022
Rule Title: Disallow AutoPlay/Autorun from Autorun.inf

Vulnerability Discussion: This registry key will prevent the autorun.inf from executing commands.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
In the Registry Editor, navigate to the following registry key:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Autorun.inf
Value Name: (Default)
Type: REG_Sz
Value: @SYS:DoesNotExist

If the above listed registry value does not exist, then this is a finding.

Fix Text: Add the registry value as specified in the manual check.

Group ID (Vulid): V-18010
Group Title: User Right - Debug Progams
Rule ID: SV-29588r1_rule
Severity: CAT I
Rule Version (STIG-ID): 4.005
Rule Title: Unapproved Users have access to Debug programs.

Vulnerability Discussion: This is a Category 1 finding as it provides access to the kernel with complete access to sensitive and critical operating system components.

Documentable: YES
Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.

Navigate to Local Policies -> User Rights Assignment.

If any user accounts, or groups, (to include administrators) are granted the “Debug programs” right, then this is a finding.

Note: Windows 2000 previously had “Administrators” listed for this User Right. If this change causes issues with your system use the Documentable and report the issue to the FSO Helpdesk at FSO_Spt@DISA.MIL.

Documentable Explanation: Some applications may require this right to function such as the Windows 2003 Cluster service account. Any exception needs to be documented with the IAO. Acceptable forms of documentation include vendor published documents and application owner confirmation.

Fix Text: Configure the system to remove any accounts from the "Debug programs" user right.

UNCLASSIFIED